

Pokročilé rysy směrovacího protokolu IS-IS

Advanced Features of IS-IS Routing Protocol

Zadání diplomové práce

Student: **Bc. Michael Waligora**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2612T025 Informatika a výpočetní technika

Téma: **Pokročilé rysy směrovacího protokolu IS-IS**
Advanced Features of IS-IS Routing Protocol

Zásady pro vypracování:

Cílem práce je prostudovat a prakticky ověřit pokročilé možnosti směrovacího protokolu IS-IS, zajistit možnost transportu generických informací a provést srovnání s protokolem OSPF.

1. Seznamte se se současným stavem standardizace směrovacího protokolu IS-IS a jeho rozšíření a popište jej.
2. Proved'te srovnání IS-IS s protokolem OSPF (mechanismus transportu směrovací informace, metrika a její rozšíření, filosofie a flexibilita realizace hierarchického směrování, rychlost konvergence). Proved'te příslušná měření na typických topologiích v laboratorním prostředí.
3. Popište a laboratorně ověřte možnosti paralelního směrování protokolů IPv4 a IPv6 včetně realizace přechodové fáze při postupném rozšiřování implementace IPv6 v síťové topologii.
4. Prozkoumejte a prakticky ověřte možnosti směrování s alternativními topologiemi (multi-topology routing) v návaznosti na implementaci QoS a současné směrování více přenosových protokolů.
5. Popište možnosti transportu generických informací v protokolových jednotkách IS-IS a jeho praktickou využitelnost. K tomuto účelu použijte, resp. upravte vhodnou otevřenou implementaci IS-IS.

Praktické ověření realizujte na platformách Cisco IOS, Linux/Quagga, popřípadě i dalších. Poskytněte kompletní dokumentaci realizovaných případových studií.

Seznam doporučené odborné literatury:

Gredler, H., Goralski, W.: The Complete IS-IS Routing Protocol. Springer-Verlag, 2010, ISBN 1-85233-822-9.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Petr Grygárek, Ph.D.**

Datum zadání: 01.09.2013

Datum odevzdání: 07.05.2014



doc. Dr. Ing. Eduard Sojka
vedoucí katedry



prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě 18. 7. 2014

.....
Kopřivnář M.

Tímto bych rád poděkoval panu Ing. Petru Grygárkovi, Ph.D. za cenné rady a připomínky při vypracování této diplomové práce.

Abstrakt

Tato diplomová práce se zabývá směrovacím protokolem IS-IS. Prvním cílem práce bylo popsání současného stavu standardizace IS-IS a porovnání IS-IS s OSPF. Práce obsahuje srovnání rychlosti konvergence IS-IS a OSPF na různých typech topologií. Dalšími cíli bylo vytvoření dvou případových studií. První studie se zabývá paralelní směrování IPv4 a IPv6, druhá studie popisuje možnosti směrování s alternativními topologiemi. Obě studie byly provedeny na směrovačích Cisco. Posledním cílem práce bylo prozkoumání možností a praktické využití přenosu generických informací v protokolových jednotkách IS-IS. K tomuto účelu byla rozšířena otevřená implementace ISISd, která je součástí směrovacího balíčku Quagga.

Klíčová slova: Alternativní topologie, IGP, IPv6, IS-IS, ISISd, OSPF, přenos generických informací, směrování

Abstract

This diploma thesis deals with IS-IS routing protocol. The first aim of this work was description of current state of standartization of IS-IS and comparison of IS-IS with OSPF. This work contains comparison of convergence speeds of IS-IS and OSPF. Another aims was creation of two case studies. The first case study deals with parallel routing of IPv4 and IPv6, the second case study describes options of multi-topology routing. Both studies was undertaken on Cisco routers. The last aim was exploration of possibilities and practical utilization of transmission of generic informations in IS-IS protocol data units. For this purpose ISISd open implementation was extended, ISISd is part of Quagga routing suite.

Keywords: Multi topology, IGP, IPv6, IS-IS, ISISd, OSPF, transmission of generic information, routing

Seznam použitých zkratk a symbolů

ABR	– Area Border Router
AFI	– Address Family Identifier
ASBR	– Autonomous System Boundary Router
CLNP	– Connectionless-mode Network Service
CSNP	– Complete Sequence Number PDU
DIS	– Designated Intermediate System
DR	– Designated Router
DoS	– Denial of Services
DSCP	– Differentiated Services Code Point
EIGRP	– Enhanced Interior Gateway Routing Protocol
ES	– End System
IETF	– Internet Engineering Task Force
IGP	– Interior Gateway Protocol
IIH	– IS-IS Hello
IP	– Internet Protocol
IS	– Intermediate System
IS-IS	– Intermediate System to Intermediate System
ISO	– International Organization for Standardization
LAN	– Local Area Network
LSA	– Link State Advertisement
LSP	– Link State PDU
LSU	– Link State Update
NET	– Network Entity Title
NLRI	– Network Layer Reachability Information
NPDU	– Network Protocol Data Unit
NSAP	– Network Service Access Point
MPLS	– Multiprotocol Label Switching
OSI	– Open Systems Interconnection

OSPF	– Open Shortest Path First
PDU	– Protocol data unit
PSNP	– Partial Sequence Number PDU
QoS	– Quality of Service
RFC	– Request for Comments
RIP	– Routing Information Protocol
SNPA	– Subnetwork Point of Attachment
SNPDU	– Subnetwork Protocol Data Unit
SPF	– Shortest Path First
SRM	– Send Routing Message
SSN	– Send Sequence Numbers
TLV	– Type-length-value

Obsah

1 Úvod	6
2 IS-IS	8
2.1 Princip protokolů stavů linek	8
2.2 Terminologie	9
2.3 Typy a struktura zpráv	9
2.4 Metrika	11
2.5 IS-IS adresování	12
2.6 Hierarchické směrování a oblasti	13
2.7 Objevování sousedů	17
2.8 Šíření směrovacích informací	20
2.9 Synchronizace databáze	24
2.10 Další rozšíření	26
3 Porovnání rychlosti konvergence IS-IS s OSPF	27
3.1 Testovací topologie a prostředí	27
3.2 Výsledky	28
4 Směrování s alternativními topologiemi	30
4.1 Případová studie	31
5 Paralelní směrování IPv4 a IPv6	36
5.1 Případová studie	36
6 Transport generických informací v PDU	42
6.1 Rozšíření pro přenos generických informací	42
6.2 Quagga a ISISd	43
6.3 Rozšíření implementace ISISd o podporu přenosu generické informace . .	45
6.4 Případová studie	50
7 Závěr	55
8 Reference	56
Přílohy	57
A Příloha na CD/DVD	58

B Vybrané zdrojové kódy

59

Seznam tabulek

1	Terminologie ISO/EITF	9
2	Typy PDU	11
3	Hodnoty časovačů IS-IS a OSPF	28
4	Výsledky rychlosti konvergence	29

Seznam obrázků

1	IS-IS zpráva	11
2	NET adresa	13
3	NET příklad	13
4	IS-IS hierarchické směrování	14
5	OSPF hierarchické směrování	16
6	IS-IS hierarchické směrování	17
7	IS-IS Hello	18
8	LSP	21
9	CSNP PDU	24
10	PSNP PDU	25
11	Testovací topologie	28
12	Směrování s alternativními topologiemi	33
13	Paralelní směrování IPv4 a IPv6	37
14	Geninfo TLV	43
15	Quagga architektura	44
16	ISISd architektura [17]	45
17	Šíření generických informací mezi úrovněmi	48
18	Testování přenosu generické informace	51
19	Zachycení TLV ve Wiresharku	54

Seznam výpisů zdrojového kódu

1	Konfigurace MTR	32
2	Aktivace IPv4 IS-IS	34
3	Aktivace MTR a IS-IS	34
4	MT traceroute	35
5	Konfigurace IPv6 v multi-topology režimu	39
6	Výpis sousedních směrovačů při rozšiřování IPv6 v topologii	40
7	Výpis IPv6 a IPv4 topologií	40
8	Cesta paketů z LAN1 do LAN2	41
9	Struktura geninfo	46
10	Struktura geninfo_db	47
11	Vytvoření nového příkazu	50
12	Konfigurace ISISd	52
13	Výpis Geninfo databáze	52
14	Výpis pravidel IPTABLES	53
15	Funkce pro vytvoření GENINFO TLV	59
16	Přijetí GENINFO TLV	60
17	Přidání pravidla do IPTABLES	61

1 Úvod

V dnešní době považuje každý člověk jako samozřejmost, že může využívat Internet ke komunikaci s miliardami uživateli po celém světě. Internet se skládá z navzájem propojených počítačových sítí založených na protokolu TCP/IP. Tyto počítačové sítě používají směrovací protokoly k tomu, aby mohli efektivně směrovat provoz od zdroje k cíli.

Tato práce se detailně zabývá směrovacím protokolem IS-IS. Vývoj protokolu začal v roce 1986, jako výzkumný projekt firmy DEC pro směrování v síťové architektuře DECNET Phase V. Později protokol převzala organizace ISO jako základní směrovací protokol pro referenční model ISO/OSI. V roce 1987 vydala specifikaci ISO 10589 [1], kde byl poprvé zmíněn název IS-IS. ISO 10589 definuje základní principy protokolu, bohužel zde není žádná zmínka o směrování IP protokolu. Podle této specifikace tedy není možné IS-IS použít pro směrování v Internetu. Jako hlavní protokol síťové vrstvy ISO považovalo CLNP (protokol podobný IP) a tudíž nezahrnulo podporu IP. V roce 1988 IETF začalo pracovat na novém protokolu, který měl nahradit směrovací protokol RIP, který byl nevhodný pro rozsáhlé sítě z důvodu omezení počtů skoků (založený na Bellman-Ford algoritmu). Rozhodlo se, že se budou paralelně vyvíjet protokoly založené na principu stavu linek: OSPF a IS-IS. Vznikly dvě pracovní skupiny (working groups) - OSPF-WG a ISIS-WG, při vývoji se obě skupiny navzájem inspirovaly a ovlivňovaly. IETF deklarovalo, že oba protokoly jsou si rovný. V roce 1990 bylo publikováno RFC 1195 [2], které rozšířilo IS-IS o podporu IPv4 (Integrated IS-IS). Od té doby téměř všechnu práci na vývoji IS-IS prováděla ISIS-WG. [3]

V druhé kapitole budou popsány principy fungování IS-IS a současný stav jeho standardizace. Dále v této kapitole bude IS-IS porovnán v základních vlastnostech s OSPF. OSPF zde není podrobně popsán, jsou popsány principiální rozdíly obou protokolů a zdůrazněny jejich výhody nebo nevýhody.

Třetí kapitola se zabývá měřením rychlosti konvergence protokolů IS-IS a OSPF na různých typech topologií.

Čtvrtá a pátá kapitola popisuje možnosti směrování s alternativními topologiemi a paralelního směrování protokolů IPv4 a IPv6. Obě kapitoly obsahují případové studie vypracované na platformě Cisco.

Poslední kapitola se zabývá přenosem generických informací v protokolových jednotkách IS-IS. IS-IS je navržen tak, že ho lze snadno rozšířit o novou funkcionalitu. V této kapitole bude popsáno rozšíření otevřené implementace IS-IS o podporu přenosu generických informací. Dále zde bude nastíněna praktická využitelnost tohoto řešení.

2 IS-IS

V této kapitole budou popsány základy IS-IS podle standardů ISO 10589 [1] a RFC 1195 [2]. Původně byl IS-IS vyvinut pro poskytování směrování v čistém OSI prostředí (pro směrování protokolu CLNP). V dnešní době se CLNP prakticky nepoužívá (většina standardu ISO 10589 je zastaralá) a převládají protokoly IPv4 a IPv6. Z toho důvodu práce neobsahuje informace týkající se CLNP a ISO prostředí a bude se věnovat pouze IP prostředí. Při čtení této diplomové práce se předpokládá základní znalost počítačových sítí a zejména směrovacích protokolů založených na stavu linek.

Většina v současnosti používaných IGP směrovacích protokolů (OSPF, RIP, EIGRP) je závislá na IP protokolu. IS-IS se od těchto protokolů odlišuje, že běží na druhé vrstvě modelu ISO/OSI. Díky tomu není závislý na verzi IP protokolu, a umožňuje směrování několika protokolů třetí vrstvy OSI modelu. V současnosti podporuje směrování hned tří protokolů: historického CLNP, IPv4, IPv6 a je snadno rozšiřitelný o další.

2.1 Princip protokolů stavů linek

IS-IS je IGP směrovací protokol založený na stavu linek (link state), tato podkapitola obecně popíše princip fungování těchto protokolů.

Charakteristikou směrovacích protokolů založených na stavu linek je, že každý směrovač zná kompletní topologii sítě ve směrovací doméně, označovanou jako topologická databáze. Nutné pro správné fungování je stejná topologická databáze na všech směrovačích. Nad databází směrovač vypočte pomocí SPF (Dijkstrova) algoritmu nejkratší cesty ke konkrétním sítím. Princip protokolů založených na stavu linek se skládá z těchto kroků: [4]

- Objevování sousedů a navázání přilehlosti (adjacency) - každý směrovač opakovaně posílá a přijímá Hello zprávy od sousedů. Pomocí tohoto protokolu směrovač hledá své sousedy a zjišťuje stav spojení mezi nimi.
- Šíření směrovací informace (flooding) - po objevení sousedů, směrovače si navzájem vymění informace o připojených sítích a jejich sousedech.
- Synchronizace topologické databáze - všechny směrovače v směrovací doméně musí mít stejnou topologickou databázi.
- Výpočet Dijkstrova algoritmu - pro zjištění nejkratších cest do konkrétních sítí, každý směrovač provede lokálně výpočet Dijkstrova algoritmu.

Jak se chová IS-IS v jednotlivých bodech je popsáno v následujících kapitolách.

2.2 Terminologie

Jelikož IS-IS je protokol původně standardizovaný organizací ISO, používá odlišnou terminologii pro na Internetu běžnější IETF termíny. Z tohoto důvodu jsou v tabulce 1 porovnány ISO a IETF termíny. Některé anglické literatury používají IETF označení, jiné ISO. V popisu funkcionality se namísto Intermediate System používá zažitý český název směrovač. Při porovnání IS-IS a OSPF zbylé termíny zůstaly nezměněny. [4]

IETF termíny	ISO termíny
Směrovač (router)	Intermediate System (IS)
Host	End System (ES)
MAC adresa	Subnetwork Point of Attachment (SNPA)
Paket	Network Protocol Data Unit (NPDU)
Rámec	Subnetwork Protocol Data Unit (SNPDU)
Link State Advertisement (LSA)	Link State PDU (LSP)
Autonomous System (AS)	Routing Domain
Backbone area	Level 2 (L2) Subdomain
Nonbackbone area	Level 1 (L1) Area

Tabulka 1: Terminologie ISO/EITF

2.3 Typy a struktura zpráv

Jak již bylo zmíněno dříve, IS-IS si vyměňuje zprávy na druhé vrstvě ISO/OSI modelu. Výhodou tohoto přístupu je, že IS-IS není zranitelný vůči externím útokům využívajících IP protokol jako např. DoS nebo spoofing. Aby útočník mohl provést útok, musel by mít přímý přístup k médiu nebo k směrovači. [4]

ISO 10589 [1] definuje 4 základní typy zpráv (PDU): IIH, LSP, CSNP, PSNP. IIH slouží k objevování sousedů a udržování přilehlosti. LSP je základním stavebním kamenem pro tvorbu databáze stavu linek. LSP je generováno každým směrovačem v síti a šíří se v síti. LSP obsahuje např. informace o dostupných sítích a jejich metrikách nebo informace o sousedech směrovače. Po té, až všechny směrovače budou mít aktuální LSP od ostatních

směrovačů v síti, můžou provést výpočet nejkratších cest do jednotlivých sítí a naplnit svojí směrovací tabulku. Poslední dva typy PDU CSNP a PSNP slouží k synchronizaci databáze mezi sousedními směrovači.

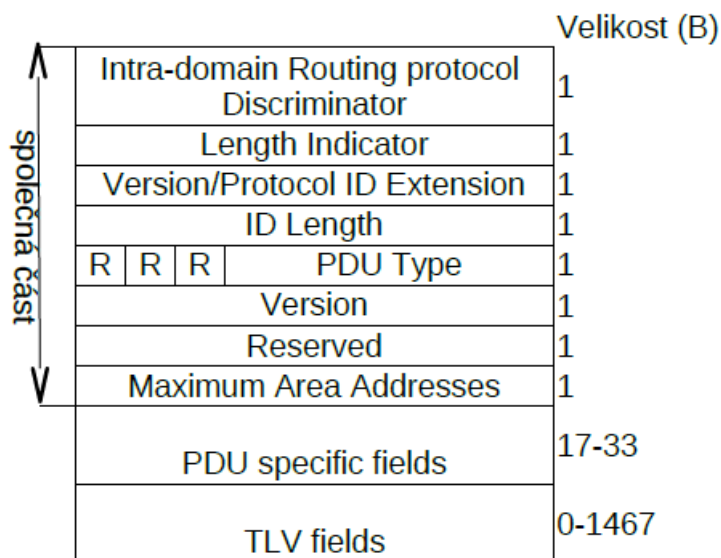
Základní struktura IS-IS zprávy je zobrazenou na obrázku 1. Všechny IS-IS zprávy začínají společnou částí o velikosti 8 bajtů. Společná hlavička obsahuje tyto políčka: [1]

- Intra-domain Routing protocol Discriminator - identifikátor síťové vrstvy přiřazený IS-IS (vždy má hodnotu 0x83).
- Length Indicator - délka hlavičky v bajtech.
- Version/Protocol ID Extension - konstanta, vždy má hodnotu 1.
- ID Length - délka System-ID v NET adrese, hodnota 0 znamená délku 6.
- PDU type - číselná hodnota indikující typ PDU (viz. tabulka 2).
- Version - konstanta, vždy má hodnotu 1.
- Reserved - vždy má hodnotu 0, ignorována při přijetí.
- Maximum Area Addresses - maximální počet oblastí povolených pro tento směrovač, hodnota 0 znamená 3 povolené adresy pro tento směrovač.

Dále následuje PDU specifická část, která se liší podle typu PDU. Zpráva je zakončená sekci proměnlivé délky skládající se z tzv. TLV. TLV je formát dat skládající se z tří políček:

- Typ (Type) - typ dat.
- Délka (Length) - délka dat (políčka Value).
- Hodnota (Value) - data do maximální velikosti 255 B.

Využívání TLV patří k největším výhodám IS-IS. Díky této vlastnosti je možné protokol snadno rozšiřovat o nové rysy. Do jednotlivých TLV je možné navíc vložit SUB-TLV, které umožňují další rozšiřitelnost protokolu. IS-IS vyžaduje, aby všechny směrovače ignorovaly neznámé TLV a přeposílaly je v nepozměněné podobě. [2]



Obrázek 1: IS-IS zpráva

Hodna políčka PDU Type	Typ PDU
15	Level-1 LAN Hello
16	Level-2 LAN Hello
17	Point-to-Point Hello
18	Point-to-Point Hello
20	Level-1 Link State PDU
24	Level-1 CSNP
25	Level-1 CSNP
26	Level-1 PSNP
27	Level-2 PSNP

Tabulka 2: Typy PDU

2.4 Metrika

Metrika je kritérium, podle kterého směrovače určují nejvýhodnější cestu do sítě. V IS-IS i OSPF se metrika označuje jako cena, která je přiřazena každému rozhraní. Cena cesty ze zdroje A do cíle B je sumou cen všech odchozích rozhraní na směrovačích. [4]

2.4.1 IS-IS metriky

RFC 1195 [2] specifikuje 4 odlišné 6-bitové metriky:

- default - jediná povinná metrika, která musí být přiřazena k rozhraní.
- delay - reprezentuje zpoždění linky.
- expense - reprezentuje náklady na užívání linky.
- error - reprezentuje pravděpodobnost vzniku chyby na lince.

Myšlenka použití čtyř metrik bylo poskytnutí základní podpory pro QoS, ale většina běžných implementací IS-IS nepoužívá jinou, než default metriku.

6-bitová metrika se ukázala jako nedostatečná v moderních sítích. Z toho důvodu RFC 5305 [11] definuje novou 32b-metriku a odstraňuje delay, expense a error metriky. Oba typy metrik se můžou používat, nutné je pouze, aby v celé směrovací doméně se používal stejný typ. Většina implementací přiřazuje metrům linky standardní hodnotu 10, což může vést k suboptimálnímu směrování. Proto je vhodné manuálně přiřadit hodnotu metriky rozhraní podle rychlosti linky.

2.4.2 OSPF metriky

Specifikace OSPF nedefinuje žádnou standardní cenu pro rozhraní. OSPF používá 16-bitovou metriku pro prefixy v jedné oblasti. Pro externí prefixy se používá 24-bitová metrika. Většina implementací používá vzorec 100Mbps/rychlost linky. Všechny linky s větší rychlostí než 100Mbps mají hodnotu 1, což opět vede k suboptimálnímu směrování. Toto omezení se dá vyřešit změnou základní rychlosti 100Mbps na vyšší. [4]

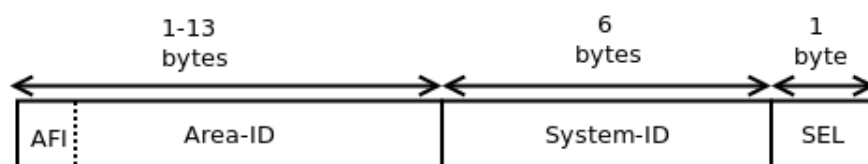
2.5 IS-IS adresování

Základním požadavkem pro správné fungování protokolů založených na stavu linek je jednoznačná identifikace směrovačů. V IS-IS má každý směrovač přiřazenou NET adresu, která je speciální verzí ISO NSAP adresy.

Obrázek 2 ukazuje strukturu NET adresy:

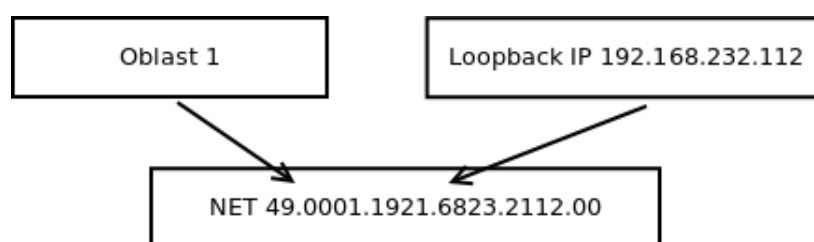
- Area-ID - určuje, do jaké oblasti směrovač náleží. První byte Area-ID je tzv. AFI. AFI identifikuje registrační autoritu adresy. Jelikož v rámci směrovací domény čísla oblastí mají lokální význam, může se použít libovolné AFI. Nejčastěji se používá AFI 49, které slouží pro privátní adresy.

- System-ID - jednoznačný identifikátor směrovače. Původní ISO norma povolovala proměnnou délku System-ID (1-8 bajtů), většina implementací však používá pevnou 6 bajtovou délku.
- Selector (SEL) - slouží k identifikaci funkce vyšší vrstvy OSI modelu, vždy musí být nastaven na 0.



Obrázek 2: NET adresa

System-ID může být libovolné 48-bitové číslo, pro snadnější zachování unikátnosti je obvyklou praxí získání System-ID z IP adresy loopbacku směrovače. Na obrázku 3 je zobrazena privátní NET adresa směrovače ležícího v oblasti 1 s Loopback adresou 192.168.232.112. [3]



Obrázek 3: NET příklad

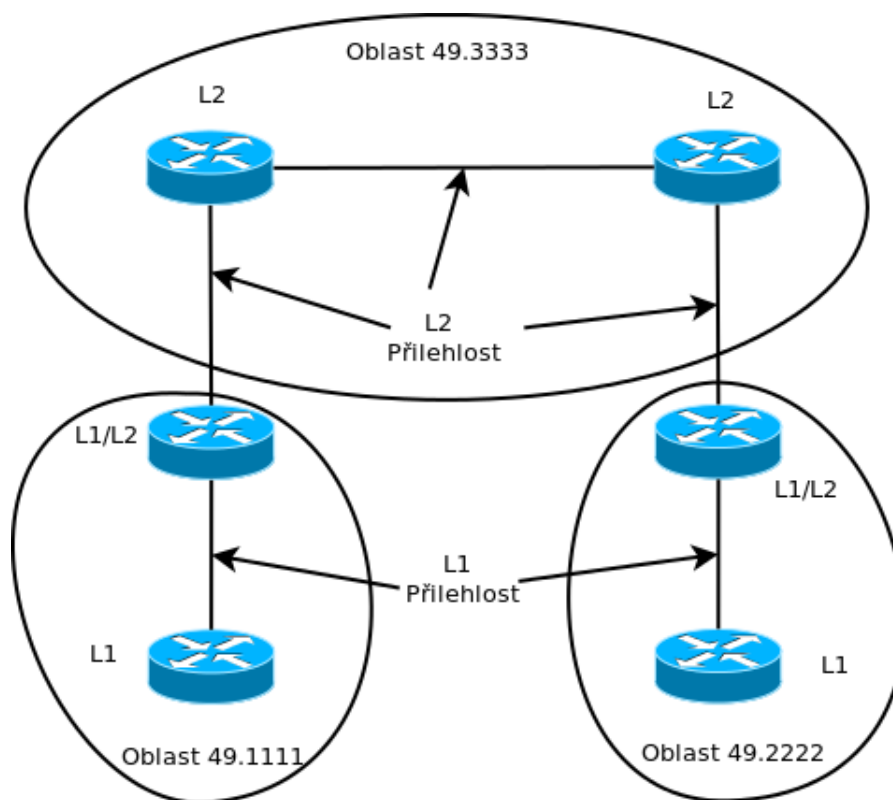
2.6 Hierarchické směrování a oblasti

S rostoucím počtem směrovačů v směrovací doméně vzniká problém s růstem velikosti databáze stavu linek a s šířením směrovacích informací. Zvyšuje se frekvence počtu oznámení o změně topologie v síti, a tudíž se častěji provádí výpočet Dijkstrova algoritmu na jednotlivých uzlech. Pokud je počet směrovačů v řádu tisíců, velikost topologické databáze o dobu výpočtu Dijkstrova algoritmu můžou způsobit vysokou zátěž procesoru směrovače. Tento problém řeší zavedení tzv. oblastí, které rozdělují síť na menší části. Směrovací informace se šíří pouze uvnitř oblasti a mezi oblastmi se šíří pouze sumární informace. Změna v jedné oblasti nevyvolá výpočet SPF v jiných oblastech a provede se

pouze lokální výpočet SPF. IS-IS i OSPF využívá dvou-úrovňovou hierarchii. V IS-IS i OSPF je síť rozdělena na tranzitní a netranzitní část. Všechny provoz mezi netranzitními částmi sítě musí procházet tranzitní částí, aby se zamezilo smyčkám. [3]

2.6.1 Hierarchické směrování v IS-IS

Hierarchické směrování je realizováno pomocí úrovní - Level-1, Level-2. Level-2 úroveň má funkci tranzitní části sítě a spojuje Level-1 oblasti. Všechny směrovače si vytvářejí pro každou úroveň vlastní topologickou databázi. Každá linka nese označení, do jaké topologie náleží - L1, L2 nebo L1/L2. Na obrázku 4 je zobrazena minimalistická topologie s jednou tranzitní Level-2 a dvěma netranzitními Level-1 oblastmi. Hranice mezi dvěma oblastmi se nachází v půlce linky mezi hraničními směrovači (L1/L2). [2] [3]



Obrázek 4: IS-IS hierarchické směrování

Nutnou podmínkou k výměně LSP je navázání přilehlosti. K vytvoření přilehlosti v Level-1 topologii se ID oblastí musí shodovat. Pro Level-2 přilehlost na ID oblasti nezáleží. Jediným omezením pro vytvoření páteří Level-2 oblasti je spojitá množina

linek přiřazených do Level-2 topologie (nemůžou existovat izolované ostrůvky páteřní sítě). [2] [3]

Šíření cest mezi úrovněmi

Standardním chováním IS-IS je, že propouští informace o cestách z Level-1 do Level-2, ale nepropouští z Level-2 do Level-1 oblastí (RFC 1195 to přímo zakazuje). L2 směrovače mají informace o všech sítích v směrovací doméně. L1 směrovače znají cesty k sítím pouze ve své oblasti a veškerý provoz ven směřují k nejbližšímu L1/L2 směrovači. [2] [3]

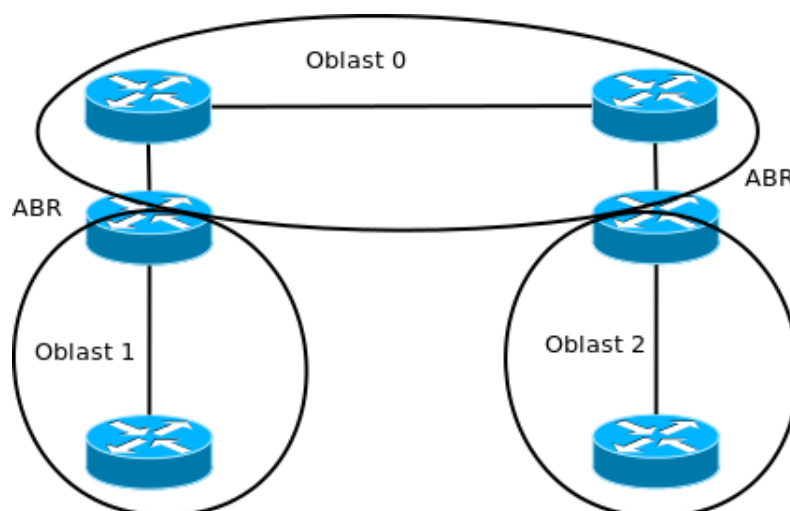
Standardní chování IS-IS při propouštění cest mezi Level-2 do Level-1 má své výhody a nevýhody. Výhodou je snížení velikosti směrovací tabulky na Level-1 směrovačích. Nevýhoda je, že pokud je v Level-1 více L1/L2 směrovačů, může docházet k suboptimálnímu směrování (Level-1 směrovač vždy posílá provoz mimo oblast na nejbližší L1/L2 směrovač bez ohledu na celkovou velikost metriky). Tento problém řeší RFC 5302 [10], které povoluje propouštění cest z Level-2 do Level-1 úrovně. Dále povoluje existenci externích cest v Level-1 úrovni.

2.6.2 Hierarchické směrování v OSPF

OSPF přistupuje k hierarchickému směrování odlišným způsobem. Na rozdíl od IS-IS, do oblasti není přiřazen směrovač, ale jeho rozhraní. Na obrázku 5 je analogická topologie k IS-IS topologii. Zde hranice mezi oblastmi jsou v půlce ABR směrovače, které se dají považovat za ekvivalent k L1/L2 směrovačů v IS-IS. Ekvivalentem k Level-2 úrovni je v OSPF páteřní oblast 0, jež spojuje ostatní netranzitní oblasti. Příležitost se naváže mezi dvěma směrovači se stejnými čísly oblastí.

Šíření cest mezi úrovněmi

Standardně v OSPF se šíří cesty mezi všemi oblastmi v autonomním systému. Což v sítích s velkým množstvím prefixů znamená velké nároky na paměť a procesor směrovače. V OSPF se netranzitní oblasti můžou nastavit do tří režimů - Stub, Totally-Stuby a Not-So-Stubby. Do Stub oblasti nejsou propagovány externí cesty z jiného autonomního systému. Totally-Stuby oblast se chová jako standardní Level-1 v IS-IS (propaguje se do ní pouze defaultní cesta). Poslední oblastí je Not-So-Stubby, která povoluje propagování externích cest z jiného směrovacího protokolu.



Obrázek 5: OSPF hierarchické směrování

2.6.3 Výhody/Nevýhody hierarchického směrování IS-IS a OSPF

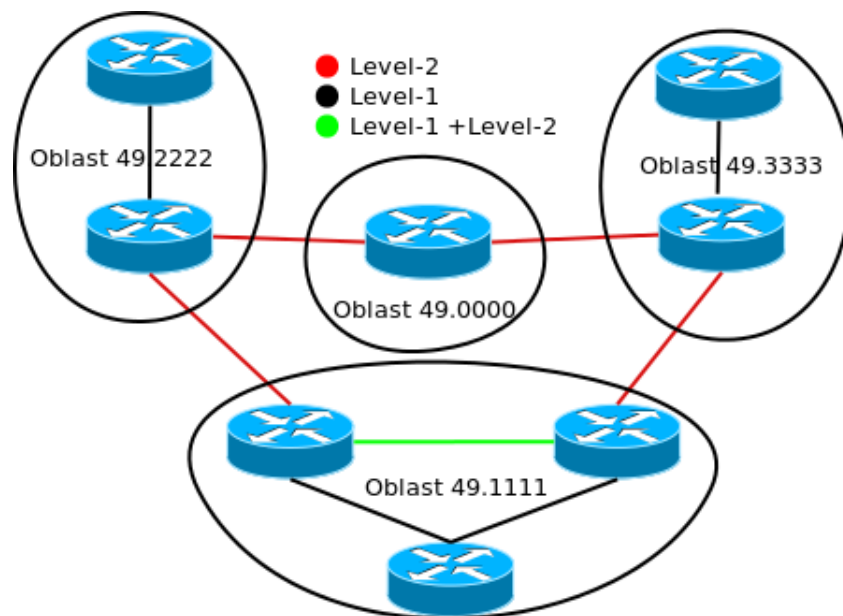
IS-IS hierarchické směrování je mnohem flexibilnější než OSPF hierarchické směrování. Obrázek 6 zobrazuje příklad IS-IS topologie, která demonstuje vlastnosti, že Level-2 úroveň se může rozkládat přes více oblastí. Další výhodou je možnost participování linky v obou topologiích (zelená linka v oblasti 49.1111). V OSPF by toto nebylo možné, a bylo by nutné přidat další linku mezi směrovači.

Poslední výhodou hierarchického směrování IS-IS je, že směrovač může být ve více oblastech zároveň. Směrovači se může přiřadit více NET adres (teoreticky až 254, prakticky se používají max. 3). Část System-ID musí být ve všech NET adresách na jednom směrovači stejná, může se lišit pouze Area-ID. Tato vlastnost má uplatnění při:

- Spojení dvou oblastí do jedné.
- Rozdělení jedné oblasti do dvou.
- Přejmenování oblastí.

Např. při spojení oblastí 49.0000 a 49.2222 do nové Level-1 oblasti 49.4444, by se na všech směrovačích v původních oblastech nastavil nový NET 49.4444.System-ID.00. Jestliže je linka mezi oběma oblastmi přiřazena také do Level-1 topologie, po odebrání původních NET adres ze všech směrovačů by vznikla nová oblast 49.4444. Při tomto postupu

by došlo ke spojení dvou oblastí bez výpadku provozu. Při navázání Level-1 příležitosti stačí, aby se alespoň jedno Area-ID shodovalo.



Obrázek 6: IS-IS hierarchické směrování

2.7 Objevování sousedů

Téměř všechny směrovací protokoly obsahují metody pro automatické objevování sousedů, které dále kontrolují, zda se poblíž nachází jiný směrovač provozující stejný směrovací protokol a zda je linka mezi směrovači průchozí v obou směrech. Pro tuto funkci používá IS-IS Hello zprávy (IIH). Celkem existují 3 typy IIH: [1]

- LAN
 - Level-1 IIH
 - Level-2 IIH
- Point-to-point IIH

LAN nebo Point-to-point IIH se generují podle typu sítě, ke které je rozhraní připojeno. U LAN sítí se IIH dělí podle toho, v jakém režimu je nastaveno rozhraní. Jestliže je rozhraní přiřazeno do Level-1 topologie, na multicastovou adresu AllL1ISs (01-80-C2-00-00-14) se posílají Level-1 IIH. Analogicky, když je rozhraní přiřazeno do Level-2 topologie, Level-2 IIH se posílají na multicastovou adresu AllL2ISs (01-80-C2-00-00-15). Každé

rozhraní může být také v obou topologiích, v tom případě se generují oba typy LAN IIH. Důvodem existence dvou LAN IIH je, že v broadcastových sítích může mít směrovač dva rozdílné sousedy pro každou topologii. Jak z názvu vyplývá, v point-to-point sítích může existovat pouze jeden soused, z tohoto důvodu je zde definován pouze jeden typ IIH. Pokud jsou v LAN sítích spojené pouze dva směrovače, je možné směrovač nastavit tak, aby linku používal jako Point-to-Point. IIH se poté posílají na multicast adresu AllIntermediateSystems (09-00-2B-00-00-05). [4]

2.7.1 PDU specifická část IIH a TLV

Na obrázku 7 jsou zobrazeny Point-to-point a LAN Hello PDU.

Point-to-Point IIH		LAN IIH		Velikost (B)
IS-IS Header		IS-IS Header		8
Reserved	Circuit Type	Reserved	Circuit Type	1
Source ID		Source ID		6
Holding Time		Holding Time		2
PDU Length		PDU Length		2
Local Circuit ID		R	Priority	1
Variable Length Fields		LAN ID		7
		Variable Length Fields		

Obrázek 7: IS-IS Hello

Význam jednotlivých polí IIH:

- Circuit Type - políčko indikuje, v jakém režimu je rozhraní nastaveno (1 - Level-1, 2 - Level-2, 3 - obě úrovně).
- Source ID - system ID odesílatele PDU.
- Holding Time - definuje maximální časový interval, po který by měl sousední směrovač čekat na IIH, než deklaruje odesílatele za mrtvého.
- PDU Length - délka IIH včetně hlavičky.
- Local Circuit ID - unikátní ID lokálního rozhraní.
- Priority - priorita směrovače používaná pro zvolení designated směrovače.
- LAN ID - identifikátor designated směrovače.

2.7.2 Designated směrovače

V broadcast sítích se navzájem vidí více zařízení. Pokud by na segmentu sítě bylo více směrovačů, synchronizace databáze a SPF výpočet by byl komplikovaný a výpočetně náročný (vznikla by full-mesh topologie). Po připojení a odpojení každého směrovače by se vygenerovalo velké množství LSP. Tento problém řeší tzv. Designated Intermediate System (DIS). DIS v topologii představuje virtuální uzel nahrazující LAN síť (místo full-mesh topologie vznikne hvězda). Všechny směrovače na LAN segmentu si synchronizují topologickou databázi pouze s DIS.

V IS-IS se volí DIS zvláště pro Level-1 i Level-2 topologii. Volba DIS je velice jednoduchá, směrovač s nejvyšší prioritou se stane DIS. Priorita může nabývat hodnot 0-127, hodnota 0 má nejnižší prioritu a hodnota 127 nejvyšší. Při rovnosti priorit rozhoduje SNPA adresa. V případě, že se v síti objeví nový směrovač s vyšší prioritou, okamžitě se stane novým DIS. Po zvolení DIS, směrovač šíří LSP reprezentující pseudonode. Rozdílem oproti klasickému LSP je v LSP-ID, které je ve formátu System-ID.X-00 (X je nenulová hodnota, v klasickém LSP je vždy 0). Původní DIS zneplatní LSP starého pseudonodu vytvořením nového LSP s políčky Lifetime and Checksum s hodnotami 0. Aby se po zvolení DIS nezvýšila cena cesty, v topologické databázi mají cesty z pseudonode cenu 0.

V OSPF se ekvivalent k DIS nazývá DR. Největším rozdílem je, že v OSPF existuje BDR (backup DR), který zastoupí funkci DR při jeho výpadku. Dále na rozdíl od IS-IS volba DR a BDR probíhá nepreemptivně (tzn. nový směrovač v síti s vyšší prioritou se nestane DR). [4]

2.7.3 Navázání příležitosti

Dva sousední směrovače formují příležitost, aby zajistily, že si můžou vzájemně spolehlivě vyměňovat směrovací informace. Dále příležitost může být myšlena jako dohoda mezi sousedy, že nastavení základních parametrů se shoduje a vyměňované informace budou správně interpretovány. V IS-IS jsou směrovače přílehlé, pokud je zajištěna obousměrná komunikace. [4]

V současnosti se na obou typech sítí k ustavení přilehlosti používá three-way-handshake. Směrovač po spuštění IS-IS procesu na rozhraní prochází třemi stavy:

- Down
- Initializing
- Up

IS-IS směrovače udržují stavy přilehlosti se sousedy v adjacency databázi. Po spuštění IS-IS procesu na rozhraní je přilehlost ve stavu Down. Nyní směrovač posílá konkrétní typ LAN IIH, ale neslyší IIH od nikoho jiného. Když směrovač uslyší příchozí LAN IIH, uloží si SNPA (MAC) adresu odesílatele. Stav se změní na Initializing a v dalších odesílaných Hello bude směrovač indikovat přijetí Hello souseda zahrnutím jeho SNPA v TLV IS Neighbour. Pokud směrovač uvidí vlastní SNPA adresu v příchozím Hello, má jistotu, že byla zajištěna obousměrná komunikace na lince a stav přilehlosti se změní na Up. [3]

Na Point-to-point linkách původní standard ISO 10589 počítal s použitím spolehlivých linek, a z toho důvodu definoval pouze two-way-handshake. Přilehlost přešla do stavu Up pokud směrovač přijímal IIH na rozhraní. Problém by mohl nastat, pokud by linka byla průchozí pouze v jednom směru. S tímto přístupem jeden systém nebude detekovat selhání, a bude směrovat provoz do nefunkční linky. Tento problém řeší RFC 5303 [12], které definuje TLV Point-to-Point Three-Way Adjacency. Princip navázání přilehlosti je stejný jako na LAN sítích. Rozdíl je, že se v TLV přenáší systémové ID namísto SNPA adresy. Obousměrná komunikace je zajištěna, pokud směrovač vidí své systémové ID v IIH sousedního směrovače. Tento přístup je kompatibilní se staršími implementacemi IS-IS, které nepodporují three-way-handshake. Při navazování přilehlosti se nově definované TLV ignoruje, a bude se používat původní two-way-handshake.

2.8 Šíření směrovacích informací

Nezbytné pro správné fungování směrovacích protokolů založených na stavu linek je stejná topologická databáze na všech směrovačích v oblasti. Toho se docílí pomocí mechanismu zaplavení (flooding) a synchronizace databáze.

2.8.1 IS-IS zaplavení

Směrovací informace se šíří prostřednictvím LSP. Účelem LSP je informovat ostatní směrovače v oblasti o stavech linek spojující přilehlé směrovače. LSP se generují např. při následujících událostech:

- Start systému.
- Navázání nebo změna stavu přilehlosti.
- Změna metriky rozhraní.
- Změna adresy oblasti, ve které se nachází směrovač.
- Změna systémového ID.
- Při vypršení periodického časovače

Po spuštění akce ze seznamu směrovač pošle LSP všem přilehlým sousedům. Směrovače po přijetí LSP ho přepošlou všem sousedům kromě toho, kdo LSP poslal. IS-IS generuje LSP pro každou úroveň zvlášť. L1 LSP jsou posílány všem Level-1 sousedům a L2 LSP všem Level-2 sousedům. [3] [1]

LSP PDU specifická část a TLV

Na obrázku 8 je zobrazen LSP. L1 a L2 LSP se od sebe liší pouze políčkem PDU Type v hlavičce.

				Velikost (B)
IS-IS Header				8
PDU Length				2
Remaining Lifetime				2
Source ID				6
Pseudonode ID				1
LSP Number				1
Sequence Number				4
Checksum				2
P	ATT	OL	IS Type	1
Variable Length Fields				

Obrázek 8: LSP

LSP-ID identifikuje konkrétní LSP a skládá se z:

- Source ID - je to hodnota systémového ID z NET směrovače, který vytvořil LSP.
- Pseudonode ID - pokud je to nenulová hodnota, LSP bylo posláno z DIS.
- LSP Number - jestliže LSP přesáhlo maximální velikost, došlo ke fragmentaci na více částí. LSP Number identifikuje konkrétní části.

Sequence Number (Sekvenční čísla) slouží k určení verze LSP. První sekvenční číslo LSP generované směrovačem má hodnotu 1 a každé další vygenerované LSP inkrementuje sekvenční číslo o jedna. Při přijetí LSP s vyšším sekvenčním číslem než má směrovač ve své databázi, je staré LSP nahrazeno novějším. Nové je přeposláno sousedům v oblasti. Při přijetí staršího LSP je příchozí LSP zahozeno. Tímto mechanismem se eliminuje možnost nainstalování do databáze starých (neplatných) informací. Jelikož je sekvenční číslo 32 bitové (4.2 miliardy LSP), v normálním provozu sítě by maximální hodnota neměla být nikdy překročena.

Funkcí políčka Lifetime (životnost) je omezení platnosti LSP v databázi. Tato vlastnost pomáhá odstranit staré a možná neplatné informace z databáze. Po vypršení Lifetime intervalu je LSP odstraněna z databáze. Každý směrovač musí periodicky obnovovat LSP před tím, než vyprší jeho životnost.

Kontrolní součet (Checksum) pomáhá odhalit porušený LSP. Je to číselná hodnota, která se vypočítává z celého paketu kromě políčka Lifetime (není konstanta a mění se v čase). [3] [1]

Pro zajištění spolehlivého zaplavení se musí provést potvrzení přijetí LSP. IS-IS používá dvě PDU - PSNP a CSNP. CSNP obsahuje hlavičky všech LSP v databázi, PSNP obsahuje pouze část hlaviček LSP v databázi. Na point-to-point linkách se používá explicitní potvrzení posláním PSNP odesílateli. V broadcast sítích se používá implicitní potvrzování. DIS periodicky vysílá CSNP. Když směrovač odešle LSP, měl by jeho popis vidět v následujícím CSNP, pokud ne, měl by LSP poslat znovu. [3]

TLV v LSP

Samotný LSP nenese žádné informace o stavu linek a topologii sítě. LSP používá osm základních TLV pro přenos těchto informací. Area Addresses a IS Neighbors byly definovány v původním ISO standardu. Area Addresses nese seznam oblastí, ve kterých se

směrovač nachází. IS Neighbors TLV obsahuje seznam přilehlých sousedů s metrikami linek, kterými jsou spojeny.

RFC 1195 následně přidalo 4 TLV pro podporu IP sítí - Protocols Supported, IP Interface Address, IP Internal Reachability Information, IP External Reachability Information. Protocols supported nese informace o podporovaných protokolech síťové vrstvy. IP Interface Address přenáší IP adresu rozhraní, z kterého bylo LSP odesláno (slouží k ujištění, že dva sousedi leží ve stejné IP síti). IP Internal Reachability Information obsahuje seznam přímo připojených sítí propagujícího směrovače a metriky jejich rozhraní. IP External Reachability Information nese informace o prefixech sítí mimo směrovací doménu IS-IS (v síti směrované jiným protokolem). Jelikož v L1 oblasti se standardně nešíří externí prefixy sítí, toto TLV se vyskytuje pouze v L2 LSP.

RFC 5305 [11] přidalo Extended IS Reachability a Extended IP Reachability TLV. Obě nové TLV mohou nést dodatečné informace v sub-TLV, které se využívají pro traffic engineering. Extended IS Reachability TLV má stejnou funkci jako IS Neighbors TLV, největším rozdílem je, že používá rozšířenou 24-bitovou metriku namísto 6-bitové. Extended IP Reachability TLV nahrazuje IP Internal a External Reachability Information TLV. Extended IP Reachability TLV používá 32-bitovou metriku namísto původní 6-bitové.

2.8.2 OSPF zaplavení

V OSPF se směrovací informace šíří přes LSU pakety, které se skládají z LSA. LSA je základní stavební prvek topologické databáze. LSU pakety se šíří pouze mezi dvěma sousedy. Pokud je nutné LSU přeposlat jinému směrovači, musí se vytvořit nové LSU. LSP se naopak šíří v celé oblasti v nezměněné podobě.

Nové LSA se generují při podobných událostech jako v IS-IS. Mechanizmy pro zajištění šíření aktuálních informací o síti, odstraňování starých LSA z databáze a zajištění integrity LSA pracují na podobném principu jako v IS-IS (hodnoty Sequence Number, Age a Checksum v LSA hlavičce).

K popisu různých typů cest slouží různé typy LSA. V OSPF tedy mají podobný význam jako LSP TLV v ISIS. LSA lze chápat více jako celý paket, obsahuje navíc sekvenční čísla, kontrolní součty, informace o směrovači apod. Základních 5 typů LSA:

- Router - propaguje připojené linky, jejich metriku a přilehlé sousedy směrovače. Šíří se v rámci oblasti.

- Network - DR na broadcast segmentu oznamuje, které směrovače jsou k němu připojeny. Šíří se v rámci oblasti.
- Network Summary - ABR propaguje pomocí tohoto LSA sumární prefixy z jiných oblastí.
- ASBR Summary - propaguje cestu k ASBR směrovači do všech oblastí.
- AS-External - šíří externí prefixy do celého OSPF autonomního systému.

OSPF také používá explicitní a implicitní potvrzování. K explicitnímu potvrzení se pošle LSack paket odesílateli LSU. Pokud směrovač uvidí své LSA v přijatém LSU, jedná se o implicitní potvrzení. [4]

2.9 Synchronizace databáze

2.9.1 Synchronizace na LAN

Jak již bylo zmíněno dříve, DIS se stará o synchronizaci databází na LAN segmentu. DIS periodicky posílá popis své databáze v CSNP PDU (interval může být od 1-65523 s). CSNP jsou posílány na adresy ALLL1IS nebo ALLL2IS podle úrovně DIS. Na obrázku 9 je zobrazen CSNP PDU.

	Velikost (B)
IS-IS Header	8
PDU Length	2
Source ID	ID Length + 1
Start LSP-ID	ID Length + 2
End LSP-ID	ID Length + 3
Variable Length Fields	

Obrázek 9: CSNP PDU

PDU Length a Source ID má stejný význam jako v LSP. Start LSP-ID a End LSP-ID slouží k popisu, zda CSNP obsahuje celou databázi DIS. Jestli celý popis databáze může být přenesen v jednom CSNP, hodnota Start LSP-ID je 0000.0000.0000.00-00 a End LSP-ID FFFF.FFFF.FFFF.FF-FF. Pokud je nutné CSNP rozdělit do více zpráv, Start LSP-ID identifikuje první položku LSP Entry TLV a End LSP-ID poslední.

LSP Entry TLV obsahuje hlavičku LSP: LSP-ID, Sequence number, Remaining lifetime a Checksum. Pomocí těchto informací se dá jednoznačně identifikovat LSP.

Každý směrovač si dále uchovává dvě značky pro každé rozhraní, které řídí šíření a potvrzování LSP: SRM (Send Routing Message) a SSN (Send Sequence Numbers). SRM indikuje, že dané LSP se musí poslat na linku. SSM indikuje, že LSP by mělo být zahrnuto v dalším PSNP. Tyto značky si uchovává každý směrovač zvlášť a nešíří se v žádném PDU.

Po přijetí CSNP každý směrovač porovná svou topologickou databázi s přijatou od DIS. Pokud má směrovač novější verzi LSP, pošle aktuální verzi na LAN segment. DIS potvrdí přijetí implicitně obsažením nového LSP v následujícím CSNP. Jestliže CSNP inzeruje novější nebo neznámé LSP, směrovač pošle DIS PSNP se svým aktuálním seznamem LSP. DIS poté pošle nejnovější verze LSP do LAN segmentu.

Obrázek 10 zobrazuje PSNP PDU. Existují opět dva typy PSNP - Level-1 a Level-2. Směrovač zahrne LSP Entry TLV k určení, jaké LSP má DIS poslat. [3] [1]

	Velikost (B)
IS-IS Header	8
PDU Length	2
Source ID	ID Length + 1
Variable Length Fields	

Obrázek 10: PSNP PDU

2.9.2 Synchronizace na Point-to-Point linkách

Na Point-to-Point linkách úvodní synchronizace začne po navázání přilehlosti. Po 3.78 - 5 sekundách směrovač zašle svůj CSNP. Náhodný interval 3.78 - 5 s se používá z důvodu spuštění směrovače v Hub and Spoke topologii, aby se Hub směrovač vyhnul zpracování velkého množství CSNP v jeden okamžik.

Jakmile směrovač obdrží CSNP souseda, porovná ho se svou databází. Pokud sousedovi nemá aktuální LSP, příjemce mu je pošle. Jakmile to udělají oba sousedé, měli by mít stejnou topologickou databázi.

Pro zajištění spolehlivosti se nastaví SRM značka pro LSP, které byly poslány. LSP se potvrzují buď explicitně PSNP, nebo implicitně v CSNP. Jakmile je LSP potvrzeno, SRM značka se vymaže. Jestliže žádné potvrzení nepřichází, směrovač periodicky přeposílá dané LSP. [3] [1]

2.10 Další rozšíření

V rámci této kapitoly jsem popsal základní principy IS-IS a prozkoumal jsem přibližně polovinu RFC dokumentů ze standardizační větve (Standards Track) IS-IS. V posledních přibližně 7 letech byl poměrně intenzivní vývoj IS-IS. IETF v této době vydala přes 20 nových RFC rozšiřující protokol. Jsou zde popsány rozšíření např. pro podporu MPLS, traffic engineering nebo pro autentizaci IS-IS PDU. Několik rozšíření se věnuje protokolům nahrazující Spanning Tree Protocol: TRILL a IEEE 802.1aq.

Rozšíření pro směrování s alternativními topologiemi, pro směrování IPv6 a přenos generických informací budou popsány podrobněji v následujících kapitolách. Seznam všech RFC týkajících se IS-IS lze nalézt zde [6].

3 Porovnání rychlosti konvergence IS-IS s OSPF

Konvergence sítě je proces synchronizace směrovacích informací po změně v topologii. Sít' je konvergovaná, když všechny směrovače mají přesný a stejný pohled na sít'. Rychlost konvergence je klíčová při poruše v síti (výpadek linky, směrovače). Pokud sít' není konvergovaná, můžou se vytvořit směrovací smyčky nebo může dojít ke ztrátě dat (obvykle vždy dojde k nějaké ztrátě dat).

Rychlost konvergence se skládá z několika faktorů:

- Rychlost detekce poruchy.
- Rychlost šíření směrovacích informací.
- Doba běhu SPF.
- Čas potřebný pro aktualizaci všech směrovacích tabulek v oblasti.

3.1 Testovací topologie a prostředí

V této kapitole je srovnána rychlost konvergence IS-IS a OSPF na typických topologiích. Na obrázku 11 jsou zobrazeny tři testovací topologie:

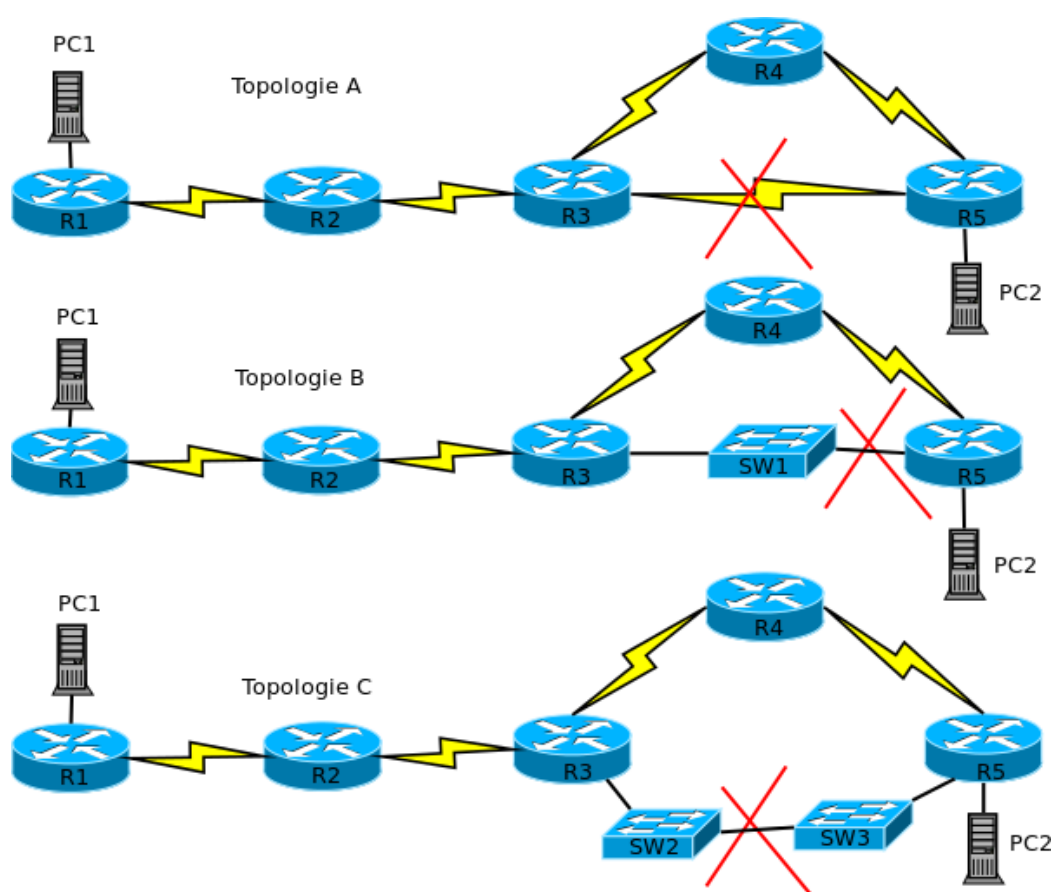
- Topologie A - v první topologii je testována rychlost konvergence při výpadku Point-to-Point linky mezi směrovači R3 a R5.
- Topologie B - druhá topologie testuje rychlost konvergence na LAN síti, k výpadku dojde mezi prvky SW1 a R5.
- Topologie C - jelikož v prvních dvou topologiích bude výpadek linky detekován hardwarem na směrovači, poslední topologie měří rychlost konvergence při výpadku spojení mezi přepínači SW2 a SW3. Směrovače budou detekovat výpadek až po vypršení časovačů.

Měření proběhlo na směrovačích Cisco 2901 s verzí IOS 15.3(2)T. Celá sít' byla nakonfigurována v jedné oblasti - IS-IS (Level-2 area), OSPF (area 0). Při měření bylo zachována standardní nastavení směrovačů, které jsou zobrazeny v tabulce 3.

K změření rychlosti konvergence jsem použil příkaz ping. Ping byl poslán z PC1 do PC2 v 0.01 s intervalech. Po výpadku linky vždy došlo ke ztrátě ICMP zpráv než sít' byla konvergovaná. Rychlost konvergence se poté zjistila vynásobením počtu chybějících ICMP zpráv velikostí intervalu.

	IS-IS		OSPF	
	Point-to-Point	Broadcast	Point-to-Point	Broadcast
Hello timer	10 s	3.3 s	10 s	10 s
Dead/Hold timer	30 s	10 s	40 s	40 s
SPF delay	5.5 s	5.5 s	5 s	5 s

Tabulka 3: Hodnoty časovačů IS-IS a OSPF



Obrázek 11: Testovací topologie

3.2 Výsledky

V tabulce 4 je zobrazena průměrná doba rychlosti konvergence. Pro každou topologii a směrovací protokol bylo provedeno 10 měření. V topologii A a B je rychlost konvergence srovnatelná u obou protokolů. Jelikož zde výpadek linky je detekován hardwarem,

velikost Dead/Hold intervalu zde nemá význam. OSPF zde má v základním nastavení 0.5 sekundovou výhodu ve zpoždění SPF výpočtu. Rychlost konvergence v topologii C závisela zejména na nastavení Hello a Dead/Hold intervalu (hardware na směrovačích R3 a R5 nedetekoval výpadek). Podle očekávání byl zde podstatně rychlejší IS-IS, který má o 30 s kratší Dead/Hold interval a vysílá Hello v 3.3 sekundových intervalech. Z tohoto důvodu jsem v Topologii C provedl druhé měření OSPF protokolu se upravenými časovači. Dead interval byl nastaven na 10 s a Hello interval na hodnotu 3 s. Rychlost konvergence OSPF s upravenými časovači byla 13.1 s. Na základě provedeného měření lze z hlediska rychlosti konvergence považovat oba protokoly za srovnatelné.

	IS-IS	OSPF
Topologie A	7,67 s	7,63 s
Topologie B	8,03 s	8,37 s
Topologie C	13,42 s	39,99 s

Tabulka 4: Výsledky rychlosti konvergence

4 Směrování s alternativními topologiemi

RFC 5120 [5] definuje rozšíření IS-IS pro provozování více nezávislých IP topologií (multi-topologií) v rámci jedné IS-IS směrovací domény. Multi-topologie (MT) mají využití ve více oblastech, jako např.:

- Udržování oddělených směrovacích domén pro části sítě IPv4 a IPv6.
- Umožnění diferenciací služeb pomocí klasifikace provozu do tříd (video, zvuk, data, ...). Provoz z každé třídy je přiřazen do určité MT a je směrován nezávisle na fyzické topologii.
- Vytvoření in-band management sítě.

MT je podmnožina směrovačů a linek fyzické topologie. Každá MT je identifikována tzv. MT ID. Na směrovači se definuje, do jakých MT jeho rozhraní náleží. Na point-to-point linkách se příležitost formuje, pokud sousedi mají alespoň jednu společnou MT. IIH obsahuje Multi-Topology TLV pro indikaci příslušnosti rozhraní k MT. Na broadcast linkách se příležitost formuje vždy bez ohledu na příslušnost v MT. To je z důvodu, aby všechny směrovače na LAN zvolily společný DIS.

RFC 5120 [5] dále definuje tři TLV, které jsou obsaženy v LSP:

- MT Intermediate System TLV - obsahuje seznam sousedů propagujícího směrovače v dané MT.
- MT Reachable IPv4 Prefixes TLV - inzeruje IPv4 prefixy připojených sítí propagujícího směrovače a jejich metriky v dané MT.
- MT Reachable IPv6 Prefixes TLV - inzeruje IPv6 prefixy připojených sítí propagujícího směrovače a jejich metriky v dané MT.

Pro každou MT se musí vypočítat vlastní SPF a jeho výsledky musí být uloženy v oddělených směrovacích tabulkách. Pokud by nebyla splněna tato podmínka, mohlo by dojít k nežádoucímu chování, jako např. k směrovacím smyčkám.

Existuje několik předdefinovaných MT ID:

- MT ID 0: ekvivalent standardní topologie.
- MT ID 1: IPv4 in-band management.

- MT ID 2: IPV6 topologie.
- MT ID 3: IPV4 multicast topologie.
- MT ID 4: IPV6 multicast topologie.
- MT ID 5: IPV6 in-band management.
- MT ID 6-3995: rezervováno pro IETF.
- MT ID 3996-4095: rezervováno pro vývoj, experimentální a proprietární vlastnosti.

4.1 Případová studie

V této případové studii bude demonstrováno využití směrování s alternativními topologiemi (multi-topology routing - MTR) pro diferenciaci služeb podle tříd provozu na platformě Cisco (konkrétně pro IPV4 unicast provoz). Konfigurace MTR se skládá z dvou hlavních kroků: definice topologie pro každou MT a klasifikaci provozu. V síti existuje základní topologie (standardní topologie, která existuje před aktivací MTR), a topologie pro specifické třídy provozu. V každé MT se šíří nezávislá množina NLRI, podle které se vypočítají oddělené směrovací tabulky.

Pro rozhodnutí, kterou MT má daný paket použít se používá 6-bitové DSCP, která je obsažena v políčku DS (Differentiated services Field) IP paketu. Paket je obvykle na vstupu do sítě označován DSCP hodnotou. Po přijetí paketu na směrovači s MTR je paket klasifikován podle DSCP hodnoty. Pokud je k dané třídě provozu přiřazena MT, provede se směrování v MT. Jestliže ve směrovací tabulce konkrétní MT není cesta k cílové síti, paket je zahozen. Jestliže třída paketu není asociována s žádnou MT, paket je směrován v základní topologii. V případě, že MTR není nakonfigurované na všech směrovačích v směrovací doméně, může se použít tzv. incremental forwarding mode, který v případě nenalezení cesty v směrovací tabulce dané MT použije směrovací tabulku základní topologie.

Existují dva MTR modely: Service Separation Model a Overlapping Model. V Service Separation Modelu se žádná MT nepřekrývá s jinou MT (pro každou třídu provozu je oddělená topologie). V Overlapping Modelu všechny MT jsou nakonfigurovány na všech směrovačích a linkách v síti a poskytuje větší redundanci než první model. Cesty pro každou třídu se v Overlapping Modelu preferují nastavením specifické metriky rozhraní dané MT. Oba modely se vzájemně nevylučují, a každý model má své výhody a nevýhody.

Jestliže dojde k výpadku na lince v MT Service Separation Modelu, neexistuje žádná alternativní cesta k cíli a provoz v dané MT bude zahazován. Naopak v Overlapping Modelu se provede nový SPF výpočet a provoz bude směrován po alternativní cestě. [7]

Cisco IOS má při směrování MT několik omezení: [7]

- Pouze unicast a multicast IPv4 MT jsou podporovány ¹.
- Všechny MT musí sdílet stejný adresní prostor (tzv. na konkrétním rozhraní nemůžou být jiné IPv4 adresy pro různé MT).
- MT nemůžou být nakonfigurovány v rámci VRF (virtual routing and forwarding).

Obrázek 12. zobrazuje ukázkou topologii. Při použití stejných metrik na linkách, by za normálních okolností docházelo k vyvažování zátěže při transportu dat z veřejné a privátní LAN do LAN1. Při použití MTR budou pakety směrovány v jednotlivých MT podle třídy provozu. V topologii existují tři unicastové třídy provozu:

- Multimediální data (DSCP 55)
- Datový provoz z veřejné LAN (DSCP 60)
- Datový provoz z privátní LAN (DSCP 55)

4.1.1 Konfigurace

Bohužel při konfiguraci MTR ve školní laboratoři jsem zjistil, že na směrovačích Cisco 2901 s verzí IOS 15.3(2)T není MTR podporováno. Z tohoto důvodu jsem k otestování funkčnosti použil síťový simulátor GNS3, který pomocí Dynamips emulátoru emuluje Cisco směrovače (k otestování byly použity směrovače Cisco 7200 s verzí IOS 12.2(33)SRE).

Konfigurační příkazy pro vytvoření MT a aktivování MTR jsou zobrazeny na výpisu 1.

```
router(config)#global-address-family ipv4 [unicast | multicast]
router(config-af)# topology <topology-name | base>

router(config)#class-map match-any <class-map-name>
```

¹Toto omezení se vztahuje pouze na definování MT pro diferenciaci služeb podle tříd provozu. Nejedná se o omezení IS-IS, ale o omezení Cisco implementace. MT pro paralelní směrování IPv4 a IPv6 jsou podporovány na platformě Cisco (viz. kapitola 5)


```
router(config-cmap)# match dscp <dscp-value>
```

```
router(config-cmap)#policy-map type class-routing ipv4 unicast <policy-map-name>
```

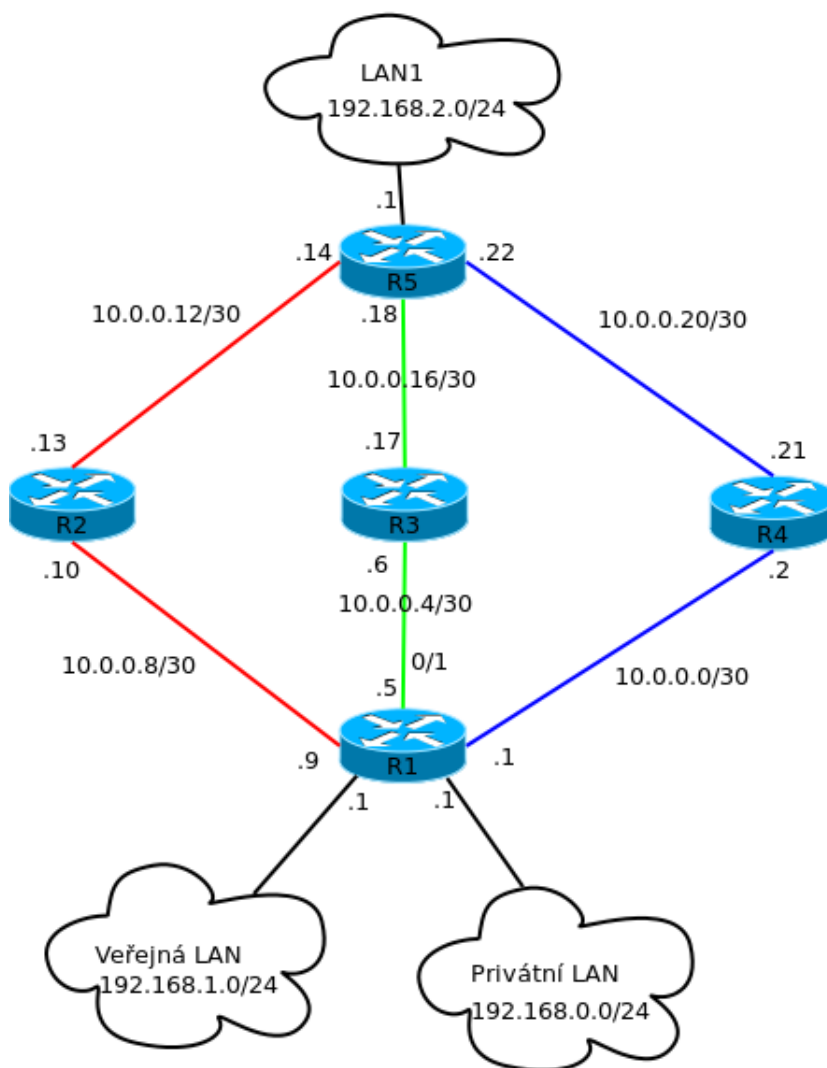
```
router(config-pmap)# class <class-map-name>
```

```
router(config-pmap-c)# select-topology <topology-name>
```

```
router(config)#global-address-family ipv4 unicast
```

```
router(config-af)#service-policy type class-routing <policy-map-name>
```

Výpis 1: Konfigurace MTR



Obrázek 12: Směrování s alternativními topologiemi

Prvními dvěma příkazy se vytvářejí nové MT. Příkazy **class-map match-any** a **match dscp** se definují class mapy, které slouží ke klasifikaci IP paketů. Příkaz **policy-map type class-routing ipv4 unicast** se vytvoří policy map, která asociuje provoz určený class mapou s MT (příkazy **class** a **select-topology**). Posledními dvěma příkazy se aktivuje MTR pro IPv4 unicastový provoz.

Na výpisu 2 jsou zobrazeny příkazy pro konfiguraci IPv4 IS-IS směrování. Příkazem **router isis** se konfiguruje IS-IS proces. Net adresa se konfiguruje příkazem **net** (příkaz může být proveden vícekrát pro přiřazení směrovače do více oblastí). IPv4 směrování na rozhraní se aktivuje příkazem **ip router isis**. **Isis circuit-type** specifikuje, v jakých úrovních bude směrovač navazovat přílehllost.

```
router(config)#router isis [process-tag]
router(config-router)#net <network-entity-title>
router(config)#interface <type> <number>
router(config-if)#ip router isis [process-tag]
router(config-if)#isis circuit-type [level-1 | level-1-2 | level-2-only]
```

Výpis 2: Aktivace IPv4 IS-IS

Konfigurační příkazy pro aktivaci MTR s IS-IS jsou zobrazeny na výpisu 3.

```
router(config)#router isis [process-tag]
router(config-router)#address-family ipv4 [unicast | multicast]
router(config-router-af)#topology <name> <tid>

router(config)#interface <type> <number>
router(config-if)#topology ipv4 <unicast | multicast>
```

Výpis 3: Aktivace MTR a IS-IS

Prvními třemi příkazy se aktivuje podpora MTR v IS-IS procesu. Příkazem **topology** se definují MT (může být vložen vícekrát), které se mají šířit v IS-IS procesu. Parametr **topology-name** musí být shodný s názvem topologie nakonfigurované výše, parametr **tid** definuje MT ID přenášené v Multi-Topology TLV. Příkazem **topology ipv4 <unicast | multicast> <topology-name>** se rozhraní přiřadí do dané MT. Všechny konfigurační soubory včetně podrobného schématu topologie jsou obsahem elektronické přílohy A.

4.1.2 Testování

K ověření správné konfigurace řešení se můžou použít následující příkazy v privilegovaném uživatelském režimu:

- **show topology detail** - vypíše detailní informace o MT.
- **show mtm table** - vypíše informace o DSCP hodnotách přiřazených k MT.
- **show ip route topology topology-name** - vypíše směrovací tabulku dané MT.
- **show isis neighbors detail** - vypíše seznam přilehlých sousedů s informacemi o použitých MT včetně MT ID.

K testování konektivity na Cisco směrovačích se můžou použít příkazy **ping topology <topology-name> <ip>** nebo **traceroute topology <topology-name> <ip>**. Výstup příkazu **traceroute** ukazuje (výpis 4), že cesta pro každou MT ze směrovače R1 do sítě LAN1 je jiná, a odpovídá dané MT.

```
R1#traceroute topology public 192.168.2.1
```

```
Type escape sequence to abort.
```

```
Tracing the route to 192.168.2.1
```

```
 1 10.0.0.10 8 msec 4 msec 12 msec
```

```
 2 10.0.0.14 4 msec * 4 msec
```

```
R1#traceroute topology multimedia 192.168.2.1
```

```
Type escape sequence to abort.
```

```
Tracing the route to 192.168.2.1
```

```
 1 10.0.0.6 4 msec 8 msec 4 msec
```

```
 2 10.0.0.18 12 msec * 28 msec
```

```
R1#traceroute topology private 192.168.2.1
```

```
Type escape sequence to abort.
```

```
Tracing the route to 192.168.2.1
```

```
 1 10.0.0.2 4 msec 4 msec 4 msec
```

```
 2 10.0.0.22 12 msec * 32 msec
```

Výpis 4: MT traceroute

5 Paralelní směrování IPv4 a IPv6

IS-IS již od RFC 1195 [2] podporuje paralelní směrování více protokolů třetí vrstvy OSI modelu (CLNP a IPv4). RFC 5308 [8] specifikuje rozšíření o podporu směrování IPv6 a definuje dvě nová TLV: IPv6 Reachability a IPv6 Interface Address.

IPv6 Reachability TLV inzeruje IPv6 prefixy přímo připojených sítí propagujícího směrovače. Používá rozšířenou 32 bitovou metriku. Obsahuje tři značky:

- U: bit indikující, zda byl prefix propuštěn do nižší úrovně.
- X: bit indikuje, zda se jedná o interní nebo externí prefix.
- S: bit indikuje, zda TLV obsahuje další Sub-TLV.

Druhé TLV IPv6 Interface Address je ekvivalentem k IP Interface Address a obsahuje IPv6 adresu rozhraní směrovače, který vytvořil dané LSP a IIH (slouží k ujištění, že dva sousedi leží ve stejné IPv6 síti). Dále RFC 5308 definovalo nové IPv6 NLPID (0x8E), kterým směrovač indikuje podporu IPv6 ve svých IIH.

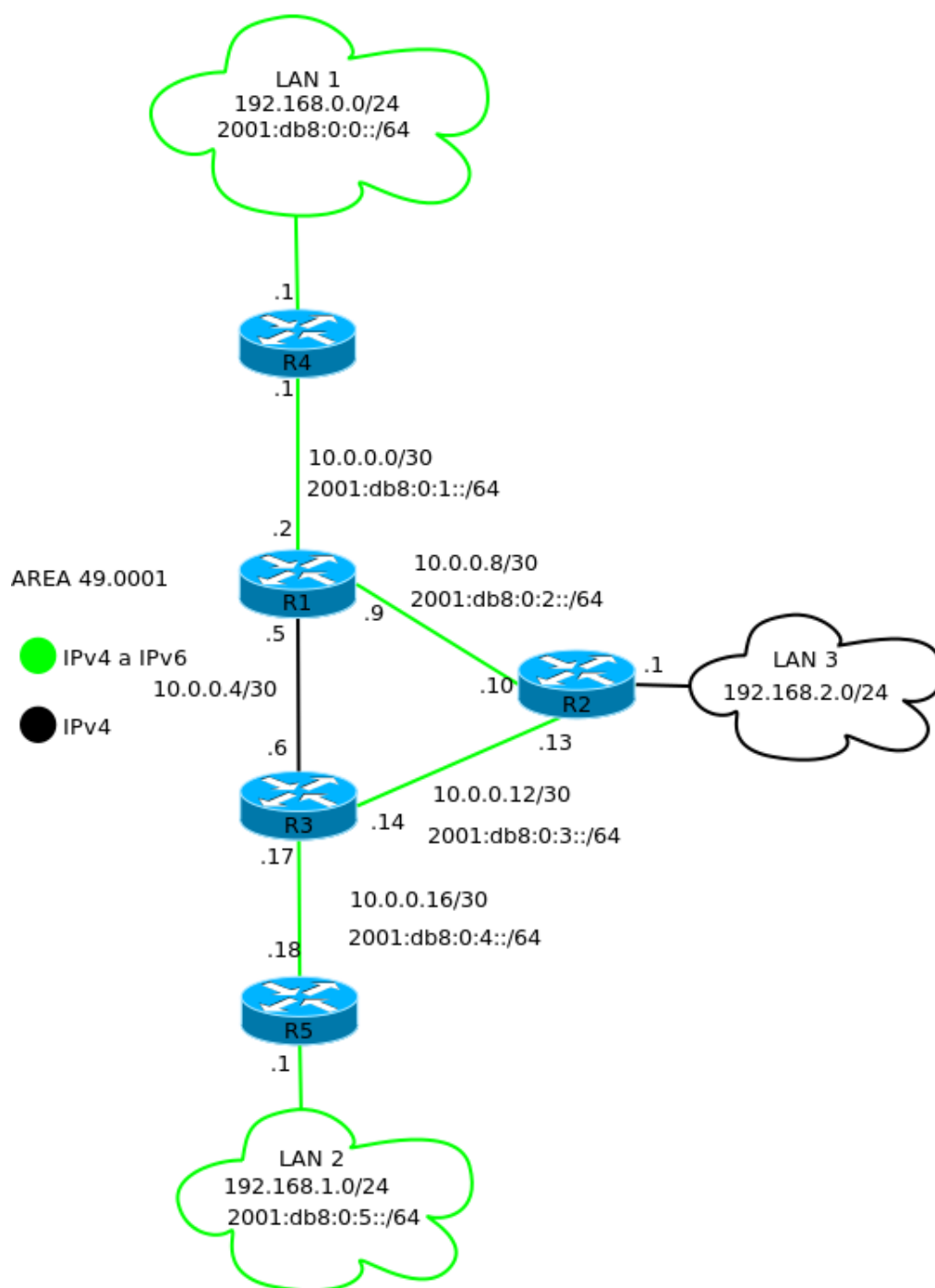
Díky těmto rozšířením může jedna instance IS-IS směrovat paralelně IPv4 a IPv6 protokoly. V případě OSPF by bylo nutné provozovat pro každý protokol vlastní instanci, což přináší zbytečné nároky jak na hardware, tak na konfiguraci.

5.1 Případová studie

V této případové studii budou popsány možnosti paralelní směrování IPv4 a IPv6 na platformě Cisco. V topologii zobrazené na obrázku 13 na všech síťových prvcích běží a je nakonfigurované IS-IS IPv4 směrování. V LAN 1 a LAN 2 jsou požadavky na zprovoznění IPv6 konektivity (vyznačena zeleně) a zachování podpory pro IPv4. V topologii se bude postupně rozšiřovat IPv6 konektivita bez výpadku IPv4 konektivity.

Cisco IOS podporuje dva režimy paralelního směrování IPv4 a IPv6:

- Single-topology (standardní režim na Cisco IOS)
- Multi-topology



Obrázek 13: Paralelní směrování IPv4 a IPv6

V režimu single-topology musí být na všech rozhraních v celé směrovací doméně nastaveny stejné protokoly třetí vrstvy (IPv4, IPv6). Tzn. že na všech rozhraních ve směrovací doméně musí být nastaveny adresy: jenom IPv4, jenom IPv6 nebo obojí. Dalším omezením je, že pro IPv4 a IPv6 musí být na rozhraní nastavena stejná hodnota metriky. Pokud je v IS-IS procesu nastaven základní typ metriky pro IPv4, Cisco směrovače nepovolí nastavení vyšší hodnoty metriky pro IPv6 prefixy (IPv6 reachability TLV podporuje pouze rozšířenou metriku).

V multi-topology režimu IS-IS udržuje nezávislé topologie pro obě protokolové rodiny, využívá k tomu rozšíření popsané v kapitole 4. Tento režim odstraňuje omezení nastavení stejných protokolových rodin na rozhraních a nutnosti použití stejné hodnoty metriky pro IPv4 a IPv6 ve směrovací doméně (vyžaduje ale použití rozšířené metriky pro IPv4).

Postupné rozšiřování IPv6 v topologii může být provedenou dvěma způsoby. Prvním způsobem je použití single-topology. Aby nedošlo k rozpadu přilehlosti a ztrátě IPv4 provozu při postupné aktivaci směrování IPv6 na rozhraní, Cisco IOS obsahuje příkaz **no adjacency-check**. Směrovače po té nebudou kontrolovat v IIR zda jeho sousedi podporují stejné protokoly třetí vrstvy. Pokud bychom tento přístup použili v této případové studii, po aktivaci IPv6 směrování v zelené části topologie by fungovala IPv4 konektivita v celé síti bez problémů. Nefungovala by však IPv6 spojení mezi LAN1 a LAN2. IS-IS předpokládá v single-topologii stejnou topologii pro obě protokolové rodiny, proto by IPv6 provoz chtěl posílat po lince mezi R3 a R2, což samozřejmě není možné. Z tohoto důvodu se v této případové studii musí použít multi-topology režim, který udržuje nezávislé topologie pro obě protokolové rodiny.

Cisco IOS podporuje ještě tzv. multi-topology transition režim, který slouží pro přechod z single-topology režimu na multi-topology režim. Pokud by se přešlo přímo na multi-topology režim, vznikly by dočasné díry v IPv6 topologii (směrovače v multi-topology režimu nerozeznají schopnost směrovačů v single-topology přenášet IPv6 provoz). Multi-topology transition režim toto řeší zahrnutím TLV v LSP pro multi i single topologie. Po rozšíření multi-topology transition režimu v celé oblasti, transition režim může být z konfigurace odebrán. [9]

5.1.1 Konfigurace MT režimu směrování IPv6

Na rozdíl od kapitoly 4, Cisco 2901 s verzí IOS 15.3(2)T ve školní laboratoři mají podporu paralelního směrování IPv4 a IPv6.

Postup při rozšiřování IPv6 v topologii se skládá z následujících kroků:

- Aktivace multi-topology režimu na všech směrovačích v směrovací doméně.
- Aktivace IPv6 směrování na daných rozhraních.

Konfigurační příkazy (předpokládá se funkční IPv4 topologie s nakonfigurovaným IS-IS procesem):

```
router(config)# ipv6 unicast-routing
router(config)#router isis [process-tag]
router(config-router)#metric-style wide
router(config-router)#address-family ipv6 unicast
router(config-router-af)#multi-topology [transition]

router(config)#interface <type> <number>
router(config)#ipv6 address <ipv6-address>/<prefix-length>
router(config-if)#ipv6 router isis [process-tag]
```

Výpis 5: Konfigurace IPv6 v multi-topology režimu

Před začátkem konfigurace IPv6 v IS-IS procesu je nutné aktivovat IPv6 směrování v globálním konfiguračním režimu příkazem **ipv6 unicast-routing**. Příkaz **metric-style wide** aktivuje používání rozšířené metriky. Podpora MT se aktivuje v konfiguračním režimu procesu IS-IS příkazy **address-family ipv6 unicast** a **multi-topology** (v případě provozování IPv6 v single-topology režimu by se tato část vypustila). Multi-topology režim se musí nastavit na všech směrovačích ve směrovací doméně před tím, než se aktivuje IPv6 směrování na rozhraních. Pokud ne, mezi směrovači nastavené v single-topology by došlo k výpadku přilehlosti. Poslední tři řádky reprezentují aktivaci IPv6 směrování na konkrétním rozhraní. Všechny konfigurační soubory včetně schématu topologie jsou obsahem elektronické přílohy A.

5.1.2 Testování

K ověření správné konfigurace řešení se můžou použít následující příkazy v privilegovaném uživatelském režimu:

- **show ipv6 protocols [summary]** - zobrazí aktivní IPv6 směrovací procesy.
- **show isis [process-tag] [ipv6 | *] topology** - zobrazí seznam propojených směrovačů ve všech oblastech.

- **show clns [process-tag] neighbors [interface-type interface-number] [area] [detail]** - zobrazí seznam sousedních směrovačů.
- **show isis ipv6 rib [ipv6-prefix]** - zobrazí lokální směrovací tabulku IS-IS procesu.

Na výpisu níže jsou zobrazeni sousedé směrovače R1 během postupného rozšiřování IPv6. I když jsou všechny směrovače nastaveny v multi-topology režimu, s některými sousedy je navázána single-topology přílehlost. To je způsobeno tím, že směrovače R2 a R3 ještě neaktivovaly IPv6 směrování na rozhraní (posílají pořád stejná IIH a LSP jako kdyby byly v single-topology). Naopak R4 již má aktivované směrování na rozhraní a indikuje to ve svých IIH a LSP.

```
R1#show clns neighbors
System Id      Interface  SNPA          State Holdtime Type Protocol
R2             Se0/1/1    *HDLC*        Up    22      L2  IS-IS
R3             Se0/0/1    *HDLC*        Up    28      L2  IS-IS
R4             Se0/0/0    *HDLC*        Up    29      L2  M-ISIS
```

Výpis 6: Výpis sousedních směrovačů při rozšiřování IPv6 v topologii

Druhý výpis ukazuje, že pro každou protokolovou rodinu IS-IS používá nezávislou topologii (cesta z R1 do R3 u IPv6 topologie nepoužívá IPv4 spojení).

```
R1#show isis topology
```

```
IS-IS TID 0 paths to level-2 routers
System Id      Metric    Next-Hop      Interface  SNPA
R1             --
R2             10       R2            Se0/1/1    *HDLC*
R3             10       R3            Se0/0/1    *HDLC*
R4             10       R4            Se0/0/0    *HDLC*
R5             20       R3            Se0/0/1    *HDLC*
```

```
R1#show isis ipv6 topology
```

```
IS-IS TID 2 paths to level-2 routers
System Id      Metric    Next-Hop      Interface  SNPA
R1             --
R2             10       R2            Se0/1/1    *HDLC*
R3             20       R2            Se0/1/1    *HDLC*
R4             10       R4            Se0/0/0    *HDLC*
R5             30       R2            Se0/1/1    *HDLC*
```

Výpis 7: Výpis IPv6 a IPv4 topologií

Poslední výpis vypisuje cestu IPv4 a IPv6 paketů z LAN1 do LAN2.

```
cnap@pcj257:~$ traceroute 192.168.1.1
traceroute to 192.168.1.1 (192.168.1.1), 30 hops max, 60 byte packets
 1  192.168.0.1 (192.168.0.1)  0.509 ms 0.510 ms 0.598 ms
 2  10.0.1.2 (10.0.1.2)  9.049 ms 13.081 ms 17.334 ms
 3  10.0.0.6 (10.0.0.6)  30.090 ms 34.244 ms 38.447 ms
 4  10.0.0.18 (10.0.0.18)  51.394 ms * *
cnap@pcj257:~$ traceroute 2001:db8:0:5::1
traceroute to 2001:db8:0:5::1 (2001:db8:0:5::1), 30 hops max, 80 byte packets
 1  2001:db8::1 (2001:db8::1)  0.665 ms 0.646 ms 0.634 ms
 2  2001:db8:0:1::2 (2001:db8:0:1::2)  14.938 ms 23.342 ms 31.756 ms
 3  2001:db8:0:2::2 (2001:db8:0:2::2)  45.525 ms 53.970 ms 62.382 ms
 4  2001:db8:0:3::2 (2001:db8:0:3::2)  76.106 ms 84.563 ms 92.960 ms
 5  2001:db8:0:4::2 (2001:db8:0:4::2)  106.671 ms 115.139 ms 123.522 ms
```

Výpis 8: Cesta paketů z LAN1 do LAN2

Během postupného rozšiřování IPv6 v topologii byl posílán ping z LAN1 do LAN2 bez ztráty paketu. Dále na směrovačích bylo zapnuté monitorování změn příležitosti (příkaz **debug isis adj-packets**) a nebyl zaznamenán výpadek příležitosti.

6 Transport generických informací v PDU

IS-IS je díky svému návrhu snadno rozšířitelný protokol. Z tohoto důvodu se dá použít i k jiným účelům, než k původně zamyšlenému směrování protokolů třetí vrstvy ISO modelu. Teoreticky může IS-IS přenášet jakýkoliv typ dat, určitě ale není vhodný např. pro přenos multimediálních dat. Přenos generický informací může být např. užitečný v těchto oblastech:

- Přenos adres druhé vrstvy OSI modelu: Toto využívají technologie TRILL [18], SPB [19] a OTV [20] pro směrování protokolů druhé vrstvy.
- Monitorování sítě a zařízení: IS-IS instance může sbírat nejrůznější data o stavech síťových prvků a distribuovat je v rámci IS-IS domény.
- Přenos konfigurací: Obecně není problém přenést konfigurační libovolných síťových aplikací.

6.1 Rozšíření pro přenos generických informací

RFC 6823 [13] popisuje způsob přenosu generické informace pomocí LSP protokolu IS-IS. Jak již bylo zmíněno dříve, v rámci LSP můžou být přenášeny tzv. TLV políčka. Typ přenášených dat je kódovaný v 8 bitech, z toho důvodu je možné přiřadit celkem 256 hodnot. Množství definovatelných hodnot pro potřeby protokolu IS-IS se ukázalo být dostatečné. Nicméně s rozšířením využívání IS-IS pro přenos informací, které nepřímou souvisí s potřebami IS-IS, způsobilo potřebu pro navýšení počtu definovaných TLV.

RFC 6823 [13] definuje nové GENINFO TLV, které se může vyskytovat v LSP. Struktura TLV je zobrazena na obrázku 14. Hodnota Type pro toto TLV je 251. Za políčkem Length následuje políčko značek (první čtyři bity jsou rezervovány):

- S: Jestliže je nastaven, TLV musí být zaplaveno přes celou směrovací doménu. Pokud ne, TLV nesmí být propuštěn mezi úrovněmi (LSP s ostatními informacemi propuštěno být může).
- D: Když je PDU s TLV propouštěno z Level-2 do Level-1 úrovně, bit musí být nastaven. Tímto se zabráňuje smyčkám.
- I: Když je nastaven, za Application ID následuje IPv4 adresa asociovaná s aplikací.
- V: Když je nastaven, za Application ID nebo IPv4 adresou následuje IPv6 adresa asociovaná s aplikací.

Application ID identifikuje aplikaci, ke které jsou vztažena generická data. V současné době IANA registruje ID 1 pro aplikaci TRILL. Za informacemi o IP adresách následuje specifická část TLV, která se definuje pro každé Application ID zvlášť.

					Velikost (B)
Type					1
Length					1
Rsvd	V	I	D	S	1
Application ID					2
Application IP Address Info					0-20
Additional Application Specific Information					0 - (252 - velikost IP Address Info)

Obrázek 14: Geninfo TLV

Operace spojené s funkcionalitou generické informace mohou negativně ovlivňovat základní účel IS-IS - směrování. Z tohoto důvodu by všechny instance využívající generické informace měly běžet v tzv. non-zero instanci [14]. Na jednom rozhraní se provozuje více instancí IS-IS (jedna instance pro generické data a jedna pro směrování), kde u každé instance je možné prioritizovat např. zpracovávání LSP, parametry šíření LSP apod.

6.2 Quagga a ISISd

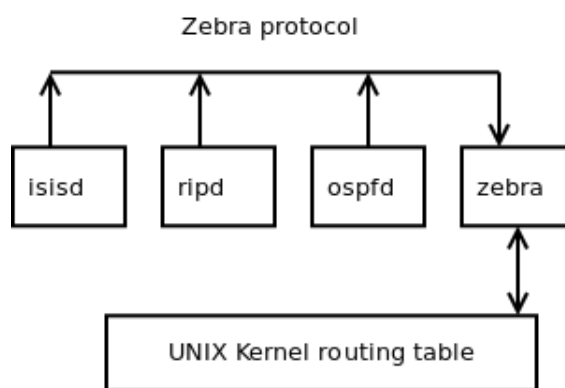
Při hledání vhodné otevřené implementace IS-IS pro rozšíření o podporu transportu generické informace jsem zjistil, že existuje pouze několik implementací IS-IS (z toho je většina proprietární). Jedinou otevřenou implementací IS-IS, která by byla vhodná pro rozšíření o podporu transportu generické informace je ISISd². Od roku 2003 je ISISd součástí projektu Quagga [15].

Před začátkem implementace rozšíření bylo nutné se seznámit s architekturami Quagga a ISISd, které budou stručně popsány v následujících podkapitolách.

²V této práci byl rozšířen modul ISISd, který je součástí Quaggy verze 0.99.22.4.

6.2.1 Quagga

Quagga je směrovací softwarový balíček dostupný pro systémy unixového typu. Obsahuje implementace směrovacích protokolů OSPFv2, OSPFv3, RIP, RIPng, BGP-4 a IS-IS. Quagga je kolekcí několika daemonů, které spolupracují a vytvářejí směrovací tabulku. Na obrázku 15 je zobrazena architektura Quaggy. Jednotliví daemoni (moduly) používají standardní socket API pro odesílání a přijímání specifických PDU. Směrovací tabulka operačního systému se aktualizuje pomocí daemona zebra, který komunikuje s jednotlivými směrovacími daemony prostřednictvím protokolu zebra. [16]



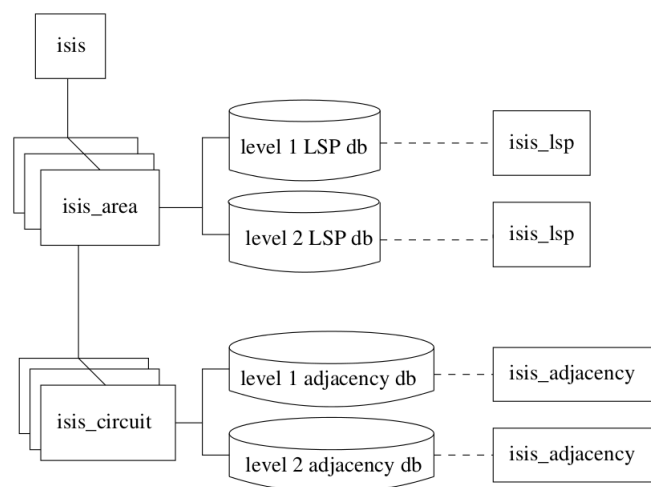
Obrázek 15: Quagga architektura

6.2.2 ISISd

ISISd je open source projekt implementace IS-IS, jehož autory jsou Sampo Saaristo, Ofer Wald, Hannes Gredler a Subbaiah Venkata. Projekt začal v roce 2001 jako modul pro GNU Zebra. Kód je napsaný v jazyce C a vydáný pod licencí GPL.

Na obrázku 16 jsou zobrazeny hlavní datové struktury ISISd a jejich vazby. Hlavní datovou strukturou celého projektu je isis (v ISISd procesu může existovat pouze jedna instance). Isis struktura obsahuje seznam IS-IS procesů (struct isis_area³) a rozhraní (struct isis_circuit). Každá oblast udržuje LSP databáze pro level-1 a level-2 úroveň. Rovněž pro každé rozhraní se udržuje databáze přilehlých směrovačů pro obě úrovně. [17]

³Název area je mírně zavádějící a nepředstavuje IS-IS oblast, ale číslo procesu.



Obrázek 16: ISISd architektura [17]

6.3 Rozšíření implementace ISISd o podporu přenosu generické informace

Pro demonstraci využitelnosti přenosu generické informace v LSP IS-IS jsem se rozhodl navrhnout aplikaci pro šíření informací o škodlivých a potencionálně nebezpečných systémech. Tento přístup může být např. užitečný při integraci IS-IS s IDS systémy. Po detekci útoku se informace o útočnickovi můžou poslat pomocí GENINFO TLV ostatním směrovačům, a přijmout bezpečnostní opatření. Při zpracovávání GENINFO TLV se nastaví firewall tak, aby nesměroval pakety se zdrojovou IPv4 adresou obsaženou v TLV.

Při rozšiřování ISISd o podporu přenosu generických informací nebylo nutné výrazněji zasahovat do architektury ISISd. Využil jsem stávajících postupů a musel jsem upravit kód týkající se generování/přijímání LSP a TLV. Téměř veškeré rozšíření kódu bylo provedeno v souborech `isis_lsp.ch`, `isis_tlv.ch` a `isisd.ch`. Nicméně zorientování se v cizím kódu, do kterého během 10 let zasahovalo několik vývojářů, nebylo úplně snadnou záležitostí.

6.3.1 Rozšíření GENINFO TLV

Pro přenos generických informací jsem využil GENINFO TLV, pro potřeby aplikace jsem v políčku Additional Application Specific Information definoval následující políčka:

- System-ID: identifikátor propagujícího směrovače (shoduje se s System-ID v IS-IS procesu). Zahrnutí System-ID v TLV je důležité při identifikaci autora TLV při šíření TLV do jiných úrovní.

- Sequence Number: 16-bitové číslo, slouží k určení verze TLV (při opakovaném přijetí generických informací směrovač nahrazuje TLV s numericky vyšším sekvenčním číslem).
- Application data: obsahuje zprávu s informativním popisem (maximální délka zprávy je 224 znaků).

Pro reprezentaci datové části TLV GENINFO jsem navrhl strukturu **geninfo** (soubor `isis_tlv.h`) zobrazenou na výpisu 9. Velikost **application_data** políčka je ovlivně omezením maximální velikostí datové části TLV (256 B). Maximální velikost **application_data** má hodnotu 224 B (256-velikost ostatních proměnných v datové části).

```

struct geninfo
{
    u_char flags;
    u_int16_t application_id;
    struct in_addr application_ipv4;
    struct in6_addr application_ipv6;
    u_char sysid[ISIS_SYS_ID_LEN];
    u_int16_t seq_num;
    u_char application_data[224];
};

```

Výpis 9: Struktura `geninfo`

6.3.2 Geninfo databáze

Teoreticky by bylo možné přijaté generické informace ukládat do LSP databáze s ostatními přijatými informacemi v LSP. Jelikož generické informace nemají vliv na standardní chování protokolu, rozhodl jsem se ukládat přijaté GENINFO TLV do logicky oddělení Geninfo databáze.

Pro uložení Geninfo databáze jsem rozšířil strukturu **isis_area** (soubor `isisd.h`) o proměnné **dict_t *geninfo_l1_db** a **dict_t *geninfo_l2_db** (`dict_t` je implementace slovníku, která je součástí ISISd). Každá proměnná udržuje seznam přijatých TLV pro každou úroveň. Jelikož pro každý IS-IS proces se vytváří vlastní instance proměnné **isis_area**, je zajištěno separátní úložiště Geninfo databáze v případě běhu více IS-IS procesů. Klíčem slovníku je System-ID propagujícího směrovače (tzn. v databázi je uložen jeden záznam GENINFO TLV pro každý směrovač).

Výpis 10 obsahuje strukturu **geninfo_db** (soubor `isis_tlv.h`), která reprezentuje jeden záznam GENINFO TLV v databázi. Při přijetí a zpracování TLV se zkopíruje políčko lifetime z hlavičky LSP. O odečítání zbývajcího času platnosti záznamu v databázi se stará funkce **lsp_tick**, která byla součástí původní ISISd implementace. Po vypršení životnosti (hodnota 0) se záznam vymaže z databáze.

```
struct geninfo_db
{
    u_int16_t lifetime ;
    struct geninfo *geninfo;
};
```

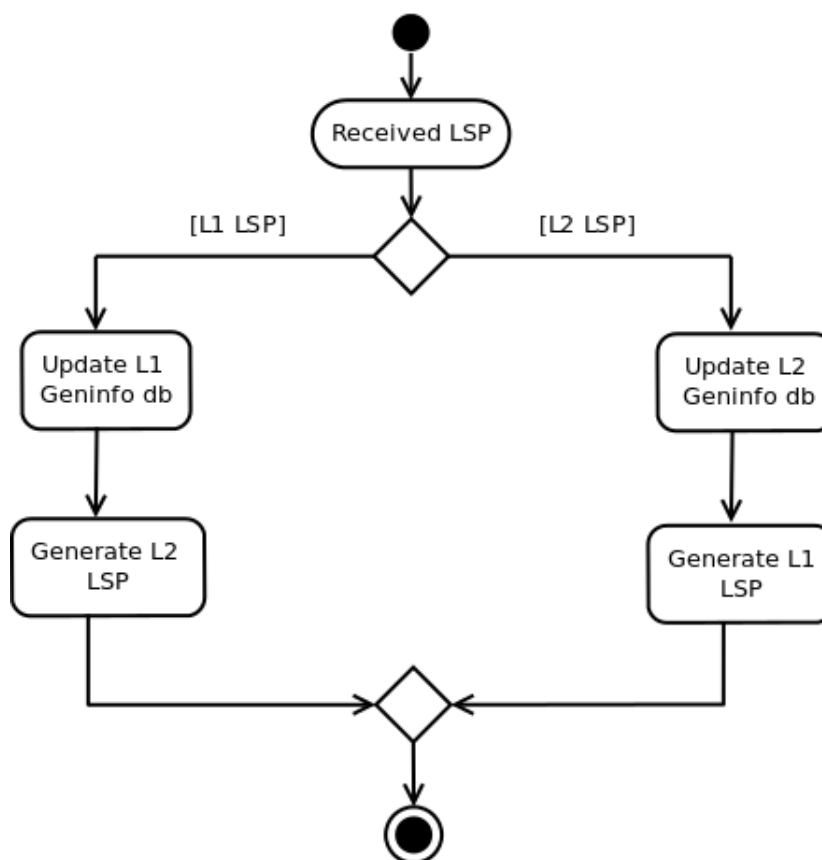
Výpis 10: Struktura `geninfo_db`

6.3.3 Šíření GENINFO TLV v LSP

Spolehlivost bezpečného přenosu generických informací zajišťují standardní mechanizmy IS-IS. Při šíření generické informace v rámci jedné úrovně není potřeba zasahovat do standardního IS-IS zaplavení. Jestliže přijaté LSP je novější, než v jeho LSP databázi, směrovač jednoduše přepošle přijaté LSP v nezměněné podobě všem sousedům v úrovni (kromě toho, kdo LSP poslal). Tímto způsobem se zajistí, že všechny směrovače v úrovni budou mít aktuální generické informace.

Pro šíření mezi úrovněmi je potřeba zajistit, aby L1/L2 směrovače zahrnuly v LSP ty GENINFO TLV, které se mají šířit po celé doméně. Tzn. v L2 LSP musí zahrnout GENINFO TLV přijaté v L1 LSP a v L1 LSP musí zahrnout GENINFO TLV přijaté v L2 LSP. Z tohoto důvodu přijaté GENINFO TLV si směrovač udržuje v databázích pro každou úroveň: L1 Geninfo db a L2 Geninfo db. Na obrázku 17 je vývojový diagram popisující chování L1/L2 směrovače při propouštění informací mezi úrovněmi. Jestliže L1/L2 směrovač přijme L1 LSP s GENINFO TLV, aktualizuje svojí L1 Geninfo databázi. Poté pokud má ve své L1 Geninfo databázi nějaké GENINFO TLV s nastaveným S bitem, vygeneruje L2 LSP obsahující tyto přijaté TLV. Při šíření informací z Level-1 do Level-2 se musí kontrolovat D značka, pokud je nastavena nesmí se TLV šířit do Level-2 úrovně.

Při přijetí L2 LSP se L1/L2 směrovač chová podobně, jako při přijetí L1 LSP. Aktualizuje svou L2 Geninfo databázi, vygeneruje L1 LSP a zahrne v něm GENINFO TLV, které mají nastavenou S značku. GENINFO TLV propouštěné z Level-2 do Level-1 se nastaví D značka. Tímto způsobem se zajistí rozšíření generických informací po celé směrovací doméně.



Obrázek 17: Šíření generických informací mezi úrovněmi

Při šíření mezi úrovněmi se využívá sekvenční číslo definované v GENINFO TLV. Např. kdyby v Level-1 oblasti byly dva L1/L2 směrovače a oba by šířily GENINFO TLV ve svých LSP. Směrovač by při přijetí těchto LSP nebyl schopen rozeznat, které GENINFO je novější.

Pokud potřebuje směrovač odebrat své GENINFO TLV z databází ostatních směrovačů, odešle LSP s GENINFO TLV, které obsahuje text *purged* v políčku **application_data**. Směrovače poté vymažou z databáze generické informace od směrovače, který poslal toto TLV. Tohoto principu se využívá při deaktivování šíření generických informací nebo při změně rozsahu šíření generických informací.

6.3.4 Vytvoření TLV

Nové LSP se vytvoří funkcí **lsp_generate(struct isis_area *area, int level)**. Tato funkce obstarává běžné rutinní operace spojené s vytvořením LSP. Z pohledu přidání nového TLV je důležitá funkce **lsp_build(struct isis_lsp *lsp, struct isis_area *area)** (soubor `isis_lsp.c`), která obstarává volání funkcí pro přidání různých TLV.

Pro přidání TLV GENINFO do LSP jsem vytvořil funkci **tlv_add_geninfos(struct list *geninfos, struct stream *stream)** (soubor `isis_tlv.c`, výpis 15). Parametry funkce je seznam GENINFO TLV a stream buffer, do kterého se zapisují data TLV (list a stream jsou generické struktury obsažené v ISISd). Při volání funkce **lsp_build** se kontroluje, jestli je isis proces nakonfigurován pro přijetí generických informací. Pokud je, zavolá se funkce **tlv_add_geninfos** a GENINFO TLV je přidáno do LSP.

6.3.5 Zpracování GENINFO TLV

Pro zpracovávání všech LSP v ISISd se používají funkce **lsp_update_data** a **parse_tlvs**. V rámci funkce **lsp_update_data** se definuje seznam očekávaných TLV, který se předává funkci **parse_tlvs**. Funkce **parse_tlvs** poté extrahuje očekávané TLV. Nakonec funkce **parse_tlvs** uloží dané LSP do databáze. Tyto dvě funkce jsem rozšířil o podporu parsování a ukládání GENINFO TLV do Geninfo databáze. Fragment kódu, který zpracovává přijaté TLV je zobrazen na výpisu 16.

6.3.6 Vytvoření příkazů pro konfiguraci

Pro snadnou konfiguraci jsem rozšířil ISISd o příkazy konfiguruující nastavení šíření generických informací. Funkcionalita vytvořených příkazů je popsána v kapitolách 6.4.2 a 6.4.3. Výpis 11 zobrazuje částečný kód pro vytvoření nového příkazu **geninfo app-id <app-id>**. Nový příkaz se vytvoří makrem **DEFUN** a registruje se funkcí **install_element**. Parametry makra **DEFUN** je název funkce, název instance struktury `cmd_element`, příkaz a nápověda funkce. Funkce **install_element** zaregistruje příkaz do konfiguračního režimu IS-IS procesu. Podrobnější popis jak se vytvářejí nové příkazy v Quagga najdete zde [21].

```

DEFUN (set_geninfo_applID,
      set_geninfo_applID_cmd,
      "geninfo_app-id_<0-65535>",
      "IS-IS_generic_information_Application_ID\n")
{
    ...
    return CMD_SUCCESS ;
}

install_element (ISIS_NODE, &set_geninfo_applID_cmd);

```

Výpis 11: Vytvoření nového příkazu

6.3.7 Nastavení firewallu

Nastavení firewallu nesouvisí přímo s šířením generických informací v LSP. Pro lepší otestování funkčnosti celého řešení a nastínění praktického využití, jsem se rozhodl implementovat jednoduché nastavení firewallu v rámci ISISd. Program nastaví firewall tak, že bude zahazovat směrované pakety se zdrojovou IPv4 adresou přijatou v GENINFO TLV.

Jako firewall jsem použil program IPTABLES. Pro přidávání a odebírání pravidel firewallu jsem vytvořil funkci **iptables_cmd(struct geninfo_db *new, char *action)** (soubor `isis_lsp.c`, výpis 17). Parametry funkce je záznam z Geninfo databáze a akce, kterou má firewall vykonat (přidání nebo odebrání záznamu). Pro přidávání a odebírání pravidel firewallu se ve funkci **iptables_cmd** volá funkce **system**⁴. Tato funkce provede libovolný linuxový příkaz (v tomto případě provede příkaz IPTABLES, který bude zahazovat směrovaný provoz z dané zdrojové adresy).

6.4 Případová studie

6.4.1 Testovací topologie

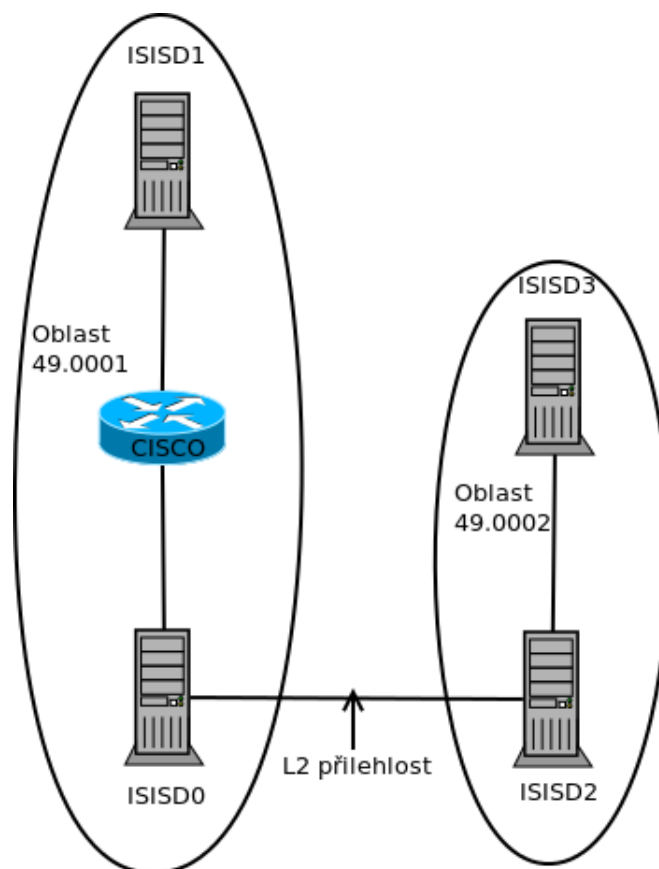
Testování funkčnosti přenosu generické informace bylo provedeno ve virtualizovaném prostředí. K virtualizaci byl použit software VirtualBox (verze 4.2.18) a GNS3 (verze 0.8.4). Ve VirtualBoxu byl nainstalován systém Ubuntu 12.10, na kterém běžel ISISd a

⁴IPTABLES nedisponují žádným stabilním otevřeným API pro C/C++ kód. Vývojáři IPTABLES doporučují použití funkce **system**. [22]

Zebra daemon. GNS3 bylo použito k emulaci Cisco směrovače a pro propojení virtualizovaných PC.

Na obrázku 18 je zobrazena topologie pro otestování funkčnosti přenosu generické informací. Sít' je rozdělena do dvou oblastí, kde v každé oblasti je mezi směrovači L1 přilehlost. Mezi počítači ISISD0 a ISISD2 je navázána L2 přilehlost, která spojuje obě oblasti. V oblasti 49.0001 je vložen emulovaný Cisco směrovač, který má ověřit, že ISIS standardně propouští neznámé TLV v nezměněném stavu.

Všichni ISISd daemoni jsou nakonfigurováni tak, že budou šířit generické informace s Application ID 10000. U každého daemona je také nastavena popisná zpráva, IPv4 a IPv6 adresa. ISISD1 a ISISD3 budou šířit své informace po celé doméně.



Obrázek 18: Testování přenosu generické informace

6.4.2 Konfigurace

ISISd používá stejnou syntaxi příkazů jako Cisco IOS⁵. Pro správné fungování musí běžet daemon Zebra. Na výpisu 12 jsou konfigurační příkazy pro konfiguraci podpory přenosu generických informací. Příkazem **geninfo app-id** se nastaví Application ID a aktivuje se podpora přenosu generických informací. Ostatní příkazy jsou volitelné a nastavují se s nimi další parametry TLV: IPv4 a IPv6 adresa, zpráva a rozsah šíření TLV. Postup instalace a konfigurační soubory včetně podrobného schématu topologie jsou obsahem elektronické přílohy A.

```

ISISD0(config)# router isis 1
ISISD0(config-router)# ge
ISISD0(config-router)# geninfo app-id <0-65535>
ISISD0(config-router)# geninfo ipv4 <ipv4-address>
ISISD0(config-router)# geninfo ipv6 <ipv6-address>
ISISD0(config-router)# geninfo message <message>
ISISD0(config-router)# geninfo scope [domain|level]

```

Výpis 12: Konfigurace ISISd

6.4.3 Testování

Pro snadnější testování šíření generické informace lze využít příkaz **generate geninfo LSP**, kterým se vygeneruje nové LSP (nemusí se čekat na standardní události IS-IS, po kterých se generuje LSP). K výpisu Geninfo databáze složí příkaz **show geninfo database**, ukázkový výstup příkazu je zobrazen na výpisu 13. ISISD0 má ve své databázi uloženy GENINFO TLV od ISISD1 (1111.1111.1111), ISISD2 (2222.2222.2222) a ISISD3 (3333.3333.3333). Tento výpis potvrzuje, že IS-IS přeposílá neznámé TLV beze změny (Cisco IOS nemá implementovanou podporu pro přenos generických informací). Obecně všechny implementace IS-IS, které neznají generické informace, budou šířit tyto informace v rámci jedné úrovně (Level-1 nebo Level-2). Problém nastane, pokud generickou informaci přijme L1/L2 směrovač, který pro ní nemá podporu. V takovém případě se informace nebudou šířit mezi úrovněmi (směrovač nezahrne GENINFO TLV přijaté v L1 LSP do L2 LSP a naopak).

```

ISISD0# show geninfo database
Geninfo L1 DB:
  Lifetime : 918
  Application ID: 10000
  System Id: 1111.1111.1111

```

⁵Konfigurační rozhraní ISISd je přístupné přes protokol telnet na portu 2608

Flags: d
 Scope: domain
 IPv4: 145.15.47.49
 IPv6: 2001::1
 Message: Dos attack

Geninfo L2 DB:

Lifetime : 1133
 Application ID: 10000
 System Id: 2222.2222.2222
 Flags: c
 Scope: level
 IPv4: 192.168.3.2
 IPv6: 11::1
 Message: Compromised server

Lifetime : 1133
 Application ID: 10000
 System Id: 3333.3333.3333
 Flags: f
 Scope: domain
 IPv4: 192.168.1.2
 IPv6: 5::5
 Message: Compromised server

Výpis 13: Výpis Geninfo databáze

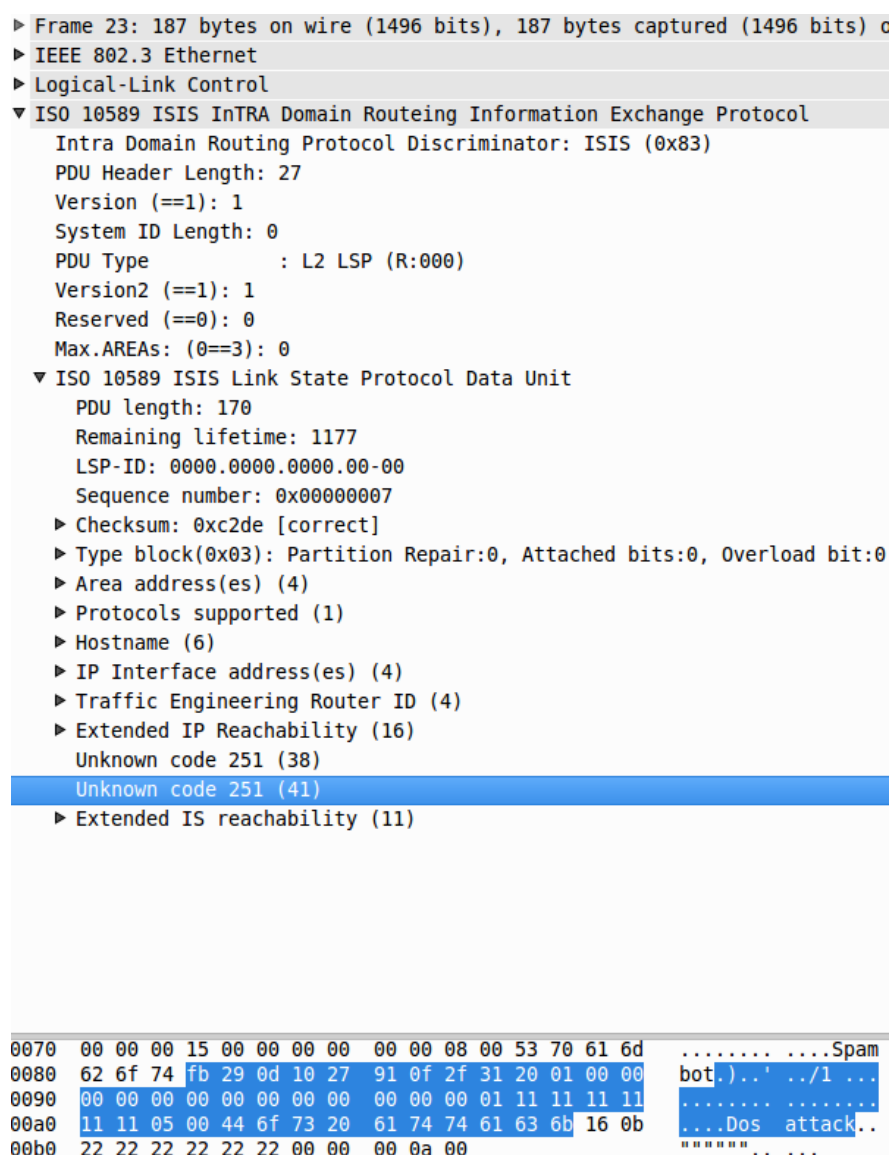
Výstup 17 zobrazuje seznam pravidel firewallu IPTABLES, který se shoduje s informacemi přijatými v GENINFO TLV. IPTABLES je nastaveno tak, že zahazuje směrovaný provoz se zdrojovou IP adresou přijatou v GENINFO TLV.

```
root@cvalin-EP45-DS3R:/home/cvalin# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination
DROP      all  --  192.168.3.2            anywhere
DROP      all  --  192.168.1.2            anywhere
DROP      all  --  145.15.47.49           anywhere
```

Výpis 14: Výpis pravidel IPTABLES

Obrázek 19 zobrazuje LSP generované ISISD0 zachycené ve Wiresharku. Wireshark nerozeznává GENINFO TLV, z tohoto důvodu poskytuje výpis pouze po jednotlivých bajtech. V tomto případě jsou v LSP obsaženy informace ze směrovače ISISD1 a ISISD0. Ve výpisu jednotlivých bajtů je vyznačeno GENINFO TLV ISISD1. První bajt reprezentuje typ TLV (251, 0xfb), druhý bajt reprezentuje délku políčka Value (41 B, 0x29). Poté následuje políčko značek. 0xd se rovná binárnímu číslu 1101, což odpovídá nastaveným značkám V, I, S (TLV obsahuje IPv4 a IPv6 adresu, šíří se v celé směrovací doméně).



Obrázek 19: Zachycení TLV ve Wiresharku

7 Závěr

Tato diplomová práce měla tři cíle: prostudování směrovacího protokolu IS-IS, praktické ověření jeho pokročilých vlastností a implementace rozšíření pro přenos generických informací v protokolových jednotkách IS-IS.

V úvodní části jsem popsal principy fungování IS-IS a provedl jsem srovnání s protokolem OSPF. Tato část byla časově asi nejvíce náročná, k prostudování a pochopení fungování IS-IS jsem musel přečíst stovky stránek RFC dokumentů a knih. Návrh IS-IS protokolu se s postupem času ukázal jako nadčasový a snadno rozšiřitelný o další funkce. Pokud se v protokolu objevily nějaké nedostatky nebo požadavky na novou funkcionalitu, protokol obvykle stačilo rozšířit o nový typ TLV a základ protokolu zůstal stejný. V této vlastnosti spočívá největší výhoda IS-IS oproti OSPF. Např. při potřebě směrování IPv6 bylo nutné vydat novou verzi OSPFv3. Zatímco specifikace rozšíření IPv6 pro IS-IS má 6 stran, specifikace OSPFv3 má 96 stran. Z pohledu primární účelu směrovacích protokolů směrování jsou oba protokoly srovnatelné. IS-IS má zde mírnou výhodu v lepší škálovatelnosti hierarchického směrování a podporu paralelního směrování více protokolů třetí vrstvy.

V části věnované případovým studiím jsem prakticky ověřil směrování s alternativními topologiemi a paralelní směrování IPv4 a IPv6 na platformě Cisco. Původně jsem chtěl vytvořit případové studie také pro platformu Linux/Quagga, ale bohužel vývoj IS-IS v rámci Quaggy není příliš podporovaný a tyto vlastnosti nejsou implementovány.

V poslední části jsem zjišťoval možnosti přenosu generických informací v protokolových jednotkách IS-IS a jeho praktickou využitelnost. K tomuto účelu jsem rozšířil modul Quaggy ISISd a vytvořil jsem aplikaci pro šíření informací o nebezpečných zařízeních v síti. Tato aplikace není určité vhodná pro ostré nasazení, ale jedná se o jakýsi prototyp, který demonstruje jakým způsobem by se měly informace šířit ve směrovací doméně. Domnívám se, že by aplikace mohla mít praktické využití, pokud by byla v budoucnu rozšířena o napojení na IDS systémy a vylepšila by se implementace nastavení firewallu.

8 Reference

- [1] ISO/IEC 10589:2002. *Intermediate System to Intermediate System intra-domain routing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service*. 2002.
- [2] CALLON, R.W. *Use of OSI IS-IS for routing in TCP/IP and dual environments: RFC 1195* [online]. IETF, 1990 [cit. 2014-06-10]. Dostupné z: <http://www.rfc-editor.org/rfc/rfc1195.txt>
- [3] GREDLER, Hannes a Walter GORALSKI. *The complete IS-IS routing protocol*. London: Springer, c2005, xvii, 540 p. ISBN 18-523-3822-9.
- [4] DOYLE, Jeff. *OSPF and IS-IS: choosing an IGP for large-scale networks*. Upper Saddle River, NJ: Addison-Wesley, c2006, xxi, 454p. ISBN 03-211-6879-8.
- [5] PRZYGIENDA, T., N. SHEN a N. SHETH. *M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems: RFC 5120* [online]. IETF, 2008 [cit. 2014-06-20]. Dostupné z: <http://www.rfc-editor.org/rfc/rfc5120.txt>
- [6] *RFC Editor* [online]. [cit. 2014-07-13]. Dostupné z: [http://www.rfc-editor.org/search/rfc_search_detail.php?page=All&title=is-is&pubstatus\[\]=Any&sortkey=Number&sorting=DESC](http://www.rfc-editor.org/search/rfc_search_detail.php?page=All&title=is-is&pubstatus[]=Any&sortkey=Number&sorting=DESC)
- [7] *Multi-Topology Routing* [online]. 2007 [cit. 2014-07-05]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/ios/12_2sr/12_2srb/feature/guide/srmtrdoc.html#wp1054794
- [8] HOPPS, C. *Routing IPv6 with IS-IS: RFC 5308* [online]. IETF, 2008 [cit. 2014-07-05]. Dostupné z: <http://www.rfc-editor.org/rfc/rfc5308.txt>
- [9] *Implementing IS-IS for IPv6* [online]. 2010 [cit. 2014-07-05]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/ios/ipv6/configuration/guide/12_4t/ipv6_12_4t_book/ip6-is-is.html
- [10] LI, T., T. PRZYGIENDA a H. SMIT. *Domain-Wide Prefix Distribution with Two-Level: RFC 5302 IS-IS* [online]. IETF, 2008 [cit. 2014-07-01]. Dostupné z: <http://www.rfc-editor.org/rfc/rfc5302.txt>
- [11] LI, T. a H. SMIT. *IS-IS Extensions for Traffic Engineering: RFC 5305* [online]. IETF, 2008 [cit. 2014-06-11]. Dostupné z: <http://www.rfc-editor.org/rfc/rfc5305.txt>

-
- [12] KATZ, D., R. SALUJA a D. EASTLAKE. *Three-Way Handshake for IS-IS Point-to-Point Adjacencies*. 2008. Dostupné z: <http://www.rfc-editor.org/rfc/rfc5303.txt>
- [13] GINSBERG, L., S. PREVIDI a M. SHAND. *Advertising Generic Information in IS-IS: RFC 6823* [online]. IETF, 2012 [cit. 2014-06-29]. Dostupné z: <http://www.rfc-editor.org/info/rfc6823>
- [14] PREVIDI, S., GINSBERG, M. SHAND, A. ROY a D. WARD. *IS-IS Multi-Instance: RFC 6822* [online]. IETF, 2012 [cit. 2014-06-29]. Dostupné z: <http://www.rfc-editor.org/rfc/rfc6822.txt>
- [15] *Quagga Routing Suite* [online]. [cit. 2014-07-13]. Dostupné z: <http://www.nongnu.org/quagga/>
- [16] ISHIGURO, Kunihiro. *Quagga: A routing software package for TCP/IP networks* [online]. 2013 [cit. 2014-07-08]. Dostupné z: <http://www.nongnu.org/quagga/docs/quagga.pdf>
- [17] SAARISTO, Sampo. *Implementation of IS-IS Routing Protocol for IP versions 4 and 6* [online]. Tampere, 2002 [cit. 2013-11-04]. Dostupné z: http://www.atm.tut.fi/faster/ipv6/isis_impl.pdf. Master of Science Thesis. Tampere University of Technology
- [18] D. Eastlake 3rd, M. Zhang, A. Ghanwani, V. Manral, A. Banerjee. *Transparent Interconnection of Lots of Links (TRILL): RFC 7180* [online]. IETF, 2014 [cit. 2014-07-14]. Dostupné z: <http://www.rfc-editor.org/rfc/rfc7180.txt>
- [19] FEDYK, D., Ed. ASHWOOD-SMITH, P. ALLAN, A. BRAGG a P. UNBEHAGEN. *IS-IS Extensions Supporting IEEE 802.1aq Shortest Path Bridging: RFC 6329* [online]. IETF, 2012 [cit. 2014-07-14]. Dostupné z: <http://www.rfc-editor.org/rfc/rfc6329.txt>
- [20] *Cisco Overlay Transport Virtualization Technology Introduction and Deployment Considerations* [online]. 2012 [cit. 2014-07-14]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/DCI/whitepaper/DCI3_OTV_Intro.pdf
- [21] *Zebra Hacking How-To* [online]. [cit. 2014-07-13]. Dostupné z: <http://www.nongnu.org/quagga/zh.html>
- [22] *Questions about netfilter development* [online]. [cit. 2014-07-08]. Dostupné z: <http://www.netfilter.org/documentation/FAQ/netfilter-faq-4.html#ss4.5>

A Příloha na CD/DVD

Součástí práce je DVD s elektronickou podobou práce ve formátu PDF/A. Dále jsou zde umístěny konfigurační soubory, schémata topologií a zdrojové kódy.

/text Elektronická podoba práce.

/case_studies Konfigurační soubory a schémata topologií případových studií.

/mt Směrování s alternativními topologiemi.

/ip46 Paralelní směrování IPv4 a IPv6.

/gen Transport generických informací .

/source Zdrojové kódy aplikace.

B Vybrané zdrojové kódy

Tato příloha obsahuje vybrané části kódu rozšíření pro přenos generických informací v LSP. Výpis 15 zobrazuje funkci `tlv_add_geninfos` (soubor `isis_tlv.c`), která přidá do LSP seznam GENINFO TLV.

```

int tlv_add_geninfos (struct list *geninfos, struct stream *stream)
{
    struct listnode *node;
    struct geninfo *geninfo;
    u_char value[255];
    u_char *pos = value;

    for (ALL_LIST_ELEMENTS_RO (geninfos, node, geninfo))
    {
        *((u_char *) pos) = geninfo->flags;
        pos += 1;
        *((u_int16_t *) pos) = geninfo->application_id;
        pos += 2;
        if (geninfo->flags & GENINFO_FLAG_I)
        {
            *((u_int32_t *) pos) = geninfo->application_ipv4.s_addr;
            pos += IPV4_MAX_BYTELEN;
        }
        if (geninfo->flags & GENINFO_FLAG_V)
        {
            memcpy(pos, &geninfo->application_ipv6.__in6_u, 16);
            pos += 16;
        }

        memcpy(pos, geninfo->sysid, ISIS_SYS_ID_LEN);
        pos += ISIS_SYS_ID_LEN;

        *((u_int16_t *) pos) = geninfo->seq_num;
        pos += 2;

        int app_len = strlen(geninfo->application_data);
        memcpy (pos, geninfo->application_data, app_len);
        pos += app_len;
    }
    return add_tlv (GENINFO, pos - value, value, stream);
}

```

Výpis 15: Funkce pro vytvoření GENINFO TLV

Výpis 16 zobrazuje fragment kódu z funkce **parse_tlv** (soubor **isis_tlv.c**), která parsuje TLV z LSP.

```
case GENINFO:
    *found |= TLVFLAG_GENINFO;

    if (*expected & TLVFLAG_GENINFO)
    {
        struct isis_area *area;
        area = isis_area_lookup(areatag);
        if (!area)
        {
            zlog_notice("Can't find ISIS instance_\n");
        }
        else
        {
            u_char *pnt2 = pnt;
            int data_length = length;

            area->geninfo_data->flags = (unsigned char*) *pnt2;
            pnt2 += 1;
            data_length -= 1;

            memcpy(&area->geninfo_data->application_id, pnt2, 2);
            pnt2 += 2;
            data_length -= 2;

            if (area->geninfo_data->flags & GENINFO_FLAG_I)
            {
                memcpy(&area->geninfo_data->application_ipv4.s_addr, pnt2, 4);
                pnt2 += 4;
                data_length -= 4;
            }
        }
    }
```

Výpis 16: Přijetí GENINFO TLV

Na výpisu 17 je funkce pro přidání pravidla IPTABLES (soubor isis_lsp.c).

```
void iptables_cmd(struct geninfo_db *new, char *action)
{
    if (new->geninfo->flags & GENINFO_FLAG_I)
    {
        char *cmd[200];
        char ipv4[INET_ADDRSTRLEN];
        snprintf (cmd, sizeof(cmd), "sudo_/sbin/iptables_-%s_FORWARD_-s_%s-j_
            DROP", action, inet_ntop(AF_INET, &new->geninfo->application_ipv4.
            s_addr, ipv4, INET_ADDRSTRLEN));
        system(cmd);
    }
}
```

Výpis 17: Přidání pravidla do IPTABLES